InfoCage モバイル防御
インストールガイド

InfoCage モバイル防御
Version 3.61
インストールガイド

はじめに

このたびは、NEC の InfoCage モバイル防御をお買い求めいただき誠にありがとうございます。InfoCage モバイル防御は、パソコンからの情報漏洩を防止するセキュリティソフトウェアです。
ご使用になる前に本書をよくお読みになり、製品の取り扱いを十分にご理解ください。

● 商標について

- 本マニュアル中のサンプル画面で使用している名称は、すべて架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

● 免責事項

本書及び本システムは、ライセンス契約に基づいて使用することができます。ライセンス契約で明示的に定められていないかぎり、日本電気株式会社は製品、及びその関連文書について、明示的にも暗黙的にも、商品性に関する保証、特定目的への適合性に関する保証、取り扱い、使用、または取引行為に伴う保証について一切の責任を負いません。

本書について

本書は、InfoCage モバイル防御を導入する手順を記載しています。InfoCage モバイル防御を導入する際にご利用ください。
また本ソフトウェアの使用に関する注意点などを記載している「2.2 注意事項」は必ずお読みください。
セットアップが完了した後は、『InfoCage モバイル防御 ユーザーズガイド』を参照してください。

本文中の記号について

本文中では、説明、操作手順の他に以下の記号を利用しています。これらの記号の意味を正しくご理解になり、本書をお読みください。

項　目	説　明
Notice	システムの取り扱いで守らなければならない事柄や特に注意すべき点、確認すべき点を説明します。
参照	関連する内容が記載されているページを紹介しています。

用語の定義

本書では、システム操作の説明に以下のような用語を用いています。
本書を確認するにあたって前提としてご理解ください。

項　目	説　明
InfoCage モバイル防御	パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。
暗号化	第三者の解読・利用を防ぐために、デジタル情報を組み替えることです。組み替えの際に用いられる特定の情報を「鍵」と呼びます。InfoCage モバイル防御はパソコンのドライブまたはフォルダを暗号化します。 メディア鍵認証方式では、鍵または合鍵などがパソコンに装着された状態、またはネットワーク鍵にアクセスできる状態のいずれかでなければ、暗号化されたハードディスクドライブの中を閲覧することはできません。 パスワード認証方式では、ユーザパスワードを認証しない限り、暗号化されたハードディスクドライブの中を閲覧することはできません。 ただし、Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。
復号	暗号化したファイルを元に戻すことです。
セキュリティ認証	パソコンを操作可能な状態にする際に、アクセスする権利があるかどうかを確認することです。セキュリティ認証を行うと、Windows へログオンしてパソコンを操作できるようになります。これによって、パソコンの不正利用やなりすまし利用を防止します。セキュリティ認証が行われないとパソコンはロックされた状態のため、パソコン内の暗号化されたデータは読み取ることができません。
InfoCage モバイル防御ユーティリティ	InfoCage モバイル防御を使ってパソコンの保護設定を行うためのアプリケーションです。InfoCage モバイル防御をパソコンにインストールして使用します。この InfoCage モバイル防御ユーティリティを起動して、パソコンの保護設定やパスワードの変更、鍵の作成（メディア鍵認証方式）の操作を行います。
メディア鍵認証方式／パスワード認証方式	InfoCage モバイル防御の運用方式です。 インストールの際に、外部メディアを鍵としてパソコンの認証を行うメディア鍵認証方式か、またはパスワードにてパソコンの認証を行うパスワード認証方式を選択します。

項　目	説　明
スーパーバイザパスワード／ユーザパスワード	InfoCage モバイル防御ユーティリティ起動時などに必要なパスワードです。メディア鍵認証方式で運用する場合はスーパーバイザパスワードを、パスワード認証方式で運用する場合はユーザパスワードを使用します。
管理者	InfoCage モバイル防御の管理者をさします。InfoCage モバイル防御のセットアッププログラムのカスタマイズを行います。
クライアント	InfoCage モバイル防御のシステム上で管理者が管理を行うパソコンをさします。
利用者	クライアントを利用する人をさします。
保護対象	暗号化によりデータを保護するパソコンの内蔵ドライブをさします。鍵を作成する際に設定します。（メディア鍵認証方式）
メディア暗号ユーティリティ	USB メモリなどのメディアの中に暗号化したファイルを保存し、これらのファイルを InfoCage モバイル防御のインストールされていないパソコンで復号し、使用するためのユーティリティです。
外部メディア自動暗号	許可された外部メディア（許可外部メディア）へ書き出すときに自動的に暗号化を行う機能です。許可外部メディアは、同じグループ名とキーワードが設定されているパソコンでのみデータを読み書き可能で、許可されていないメディアや他のグループのパソコンではデータの読み書きはできません。
外部メディア	OS がリムーバブルメディアと認識するメディア、フロッピーディスクおよび許可外部メディアのことをさします。
許可外部メディア	外部メディア自動暗号機能によりグループ内で使用が許可されたメディア（CD-R/RW、DVD-R/+R/RW/RAM は対象外）をさします。

目 次

第1章 InfoCage モバイル防御について

InfoCage モバイル防御は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。
InfoCage モバイル防御では、インストール時にパソコンを使用する人を認証する「鍵」の作成、または「パスワード」の設定を行い、保護が必要なドライブまたはフォルダの暗号化を行います。
本インストールガイドにしたがってそれぞれ設定を行ってください。
インストール後はパソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてからインストールしてください。

⚠Notice

InfoCage モバイル防御には、メディア鍵でセキュリティ認証を行う「メディア鍵認証方式」と、パスワードでセキュリティ認証を行う「パスワード認証方式」があります。
「メディア鍵認証方式」と「パスワード認証方式」の併用はできません。

1.1 InfoCage モバイル防御の特徴

InfoCage モバイル防御は、以下の機能で情報を強固に保護します。

各機能の操作方法については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

● **パソコンのロック**

メディア鍵認証方式の場合

鍵となるメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにします。
また、鍵をパソコンに装着することでセキュリティ認証が行われ、パソコンのロックを解除できます。

パスワード認証方式の場合

InfoCage モバイル防御のユーザパスワードが正しく入力された場合にセキュリティ認証が行われ、Windows にログオン可能になります。
また FeliCa カードで認証することもできます。(WindowsXP/2000 のみ)

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **ドライブ、フォルダの暗号化**

InfoCage モバイル防御は、ドライブおよびフォルダ単位で一括して内蔵ドライブ内のデータの暗号化を行います。セキュリティ認証が行われないとパソコン内のデータは暗号化されたままのため、読み取ることができません。

メディア鍵認証方式の場合

鍵となるメディアが装着された場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

パスワード認証方式の場合

パスワードを正しく入力した場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **外部メディア自動暗号** (InfoCage モバイル防御の管理者による設定が必要)

外部メディア内のデータの暗号化を自動的に行います。所属するグループ内でのみ使用が許可される外部メディア(許可外部メディア)を設定し、この許可外部メディアへはデータは自動的に暗号化されて書き込まれ、読み込むときには自動的に復号されます。

● **メディア暗号ユーティリティ**

USB メモリなどのメディアの中に暗号化して保存したファイルを、InfoCage モバイル防御のインストールされていないパソコンで復号する場合には、メディア暗号ユーティリティを使います。

● **データの抜き取り防止** （メディア鍵認証方式のみ）

認証されていないメディアへのコピーを禁止して、情報の抜き取りを防止します。

● **セキュリティチップ（TPM）でのセキュリティ強化** （InfoCage モバイル防御の管理者による設定が必要）

InfoCage モバイル防御をパスワード認証方式で運用し、セキュリティチップ（TPM）搭載のパソコンをお使いの場合、セキュリティチップ（TPM）と連携し、より強固なセキュリティを実現します。
（WindowsXP のパスワード認証方式のみ）

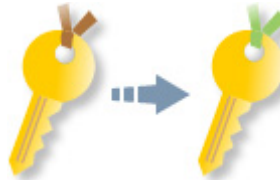
1.2 鍵とは

InfoCage モバイル防御 メディア鍵認証方式で使用する鍵には以下の 3 種類があります。

- **鍵**

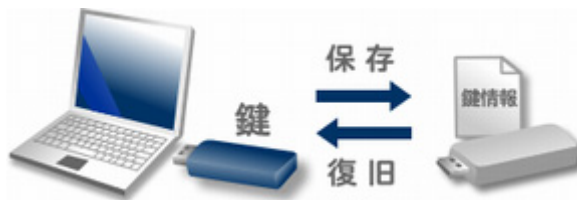
鍵とは、パソコンにログオンする際や暗号化されたデータにアクセスする際などに必要な認証情報をメディア等に作成したものです。
鍵がなければドアが開かないのと同様に、鍵として設定したメディアがなければ、セキュリティ認証が行われず、パソコンの情報にアクセスできません。
鍵はメディアやネットワークの共有フォルダに作成できます。

- **合鍵**

合鍵とは、スペアキーのことです。
万が一の鍵の紛失等に備えて、パソコンの保護対象ごとに 1 つの鍵に対して合鍵を 2 つまで作成できます。
鍵または合鍵のうちどれか 1 つで、パソコンやメディアの保護と解除ができます。

- **合成鍵**（WindowsXP／2000 のみ）

異なるメディアに作成した鍵を 2 つ組み合わせて使用するダブルロックキーのことです。
組み合わせることができるのは 2 つまでです。
鍵が 2 つそろわなければパソコンや外部メディアの保護を解除できません。

1.3 鍵情報とは

鍵のバックアップデータを鍵情報といい、鍵となるメディアとは別のメディアに保存しておきます。
鍵となるメディア内のデータを紛失した場合等は、鍵情報を元に鍵を復旧します。

> **⚠ Notice**
>
> 鍵情報を紛失すると鍵の復旧ができません。鍵情報を保存したメディア内のデータを絶対に紛失しないように注意してください。

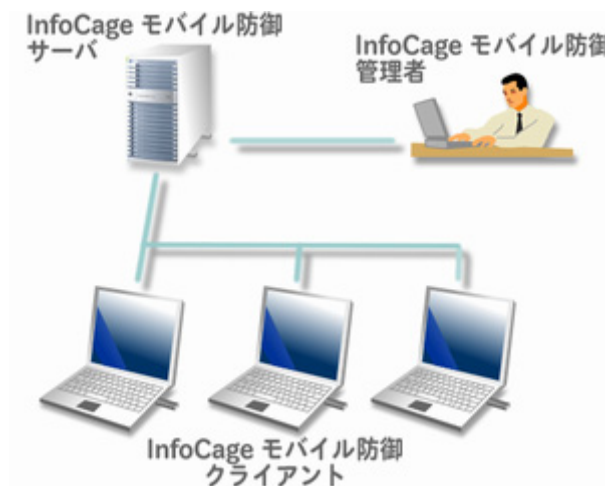
1.4 運用モード

運用モードには、クライアント単体で運用するスタンドアローンモードと、InfoCage モバイル防御の管理者が InfoCage モバイル防御サーバを使ってクライアントの設定などを管理するネットワークモードがあります。
インストール後に運用モードを変更する場合は、運用モード設定ユーティリティを使います。

● スタンドアローンモード

クライアント単体で運用します。

● ネットワークモード

スタンドアローンモードの機能に加え、InfoCage モバイル防御サーバと連携する運用モードです。
InfoCage モバイル防御の管理者が InfoCage モバイル防御サーバにてユーザ登録やポリシー設定を行い、クライアントの管理などを行います。

1.5 初期暗号化モード

InfoCage モバイル防御をインストールした後に実行される暗号化は、通常は｢ドライブ一括暗号モード｣によりドライブ単位で行われます。
ただし、InfoCage モバイル防御の管理者により｢個別暗号モード｣に設定されている場合は、指定したドライブおよびフォルダのみ暗号化を行います。
インストールする InfoCage モバイル防御の初期暗号化モードをあらかじめ InfoCage モバイル防御の管理者に確認してください。

● **ドライブ一括暗号モード （デフォルト）**

● **個別暗号モード**

第2章　インストールの前にお読みください

InfoCage モバイル防御は以下の流れでインストールします。

2.1　インストールの流れ

1. セットアッププログラムのカスタマイズ（InfoCage モバイル防御の管理者が設定）

2. 利用者にセットアッププログラムを配布

3. インストール

InfoCage モバイル防御をインストールします。

参照 インストール手順は、「3.3 Step1」を参照してください。

4. 再起動

InfoCage モバイル防御のインストール後は、ログオン方法が変わります。

参照 ログオン方法は、「3.4 Windowsへログオン」を参照してください。

5. 暗号化ウィザード

・パソコンの鍵および鍵情報を作成します。(メディア鍵認証方式のみ)
・フォルダ／ドライブを暗号化します。

参照 ドライブ一括暗号モードの場合　→　3.5 Step
個別暗号モードの場合　→　第 4 章　個別暗号モードインストール

6. 終了

⚠ Notice

InfoCage モバイル防御の管理者によってセットアッププログラムがカスタマイズされた場合は、上記の手順と異なる場合があります。

2.2 注意事項

● お願い

- インストールを行う前に、「2.3【導入前の注意事項】確認チェックシート」を使用して、インストール環境の確認を行ってください。
- 万が一に備え、大切なデータはバックアップを取ってから使用してください。

● 動作環境

<table>
<tr><th>オペレーティングシステム (*1) (*2)</th><th>システムメモリ</th><th>ハードディスクの空き容量
(インストール時)</th></tr>
<tr><td>Windows Vista Ultimate</td><td rowspan="2">1GB 以上</td><td rowspan="3">本製品のインストールドライブには45MB 以上の空き容量が必要です。
インストールの際にはセットアップ情報を展開するために、さらに 30MB 以上の空き容量が必要です。</td></tr>
<tr><td>Windows Vista Business</td></tr>
<tr><td>Windows Vista Home Basic</td><td>512MB 以上</td></tr>
<tr><td>Windows XP Professional</td><td rowspan="6">128MB 以上</td><td rowspan="6">本製品のインストールドライブには25MB 以上の空き容量が必要です。
インストールの際にはセットアップ情報を展開するために、さらに 20MB 以上の空き容量が必要です。</td></tr>
<tr><td>Windows XP Home Edition</td></tr>
<tr><td>Windows XP Tablet PC Edition</td></tr>
<tr><td>Windows XP Tablet PC Edition 2005</td></tr>
<tr><td>Windows 2000 Professional</td></tr>
<tr><th colspan="3">ハードディスクの空き容量(暗号化時)</th></tr>
<tr><td colspan="3">暗号化する際には、以下の空き容量が必要です。
必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋(ドライブ容量×0.02)
(上記は最低限必要な容量です。暗号化処理は十分な空き容量がある状態で行ってください。)
メディア鍵認証方式の場合、初めて暗号化処理を行う場合は、保護対象に指定したドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。</td></tr>
</table>

(*1) 32bit 版の日本語オペレーティングシステムをサポートしています。
(*2) Microsoft 社から提供される最新セキュリティパッチの適用をお奨めします。

● インストール前の注意事項

- InfoCage モバイル防御を Windows XP または Windows2000 で使用している場合、Windows Vista 用のセットアッププログラムを使用してアップグレードインストールすることはできません。また、その逆も同様です。
- InfoCage モバイル防御と共存できないアプリケーションと併用すると、正しく動作しない場合があります。インストール前に「アプリケーション競合問題について 」を必ず確認してください。
- インストールは、コンピュータの管理者権限を持つユーザで、日本語または英語以外の文字を含まないユーザ名で行ってください。
  InfoCage モバイル防御 ユーティリティの操作もコンピュータの管理者で行ってください。
  また、Windows XP の[別のユーザとして実行]機能、Windows Vista の[管理者として実行]機能は、使用しないでください。
- Windows Vista の場合、インストールの前にユーザアカウント制御(UAC)は有効にしてください。
  ユーザアカウント制御(UAC)の設定は、コントロールパネルの[ユーザアカウントの変更]より[ユーザアカウント制御の有効化または無効化]で行います。
  また、インストール後もユーザアカウント制御(UAC)は常に有効にしてください。

- プロダクト ID はライセンス証書に記載されています。
- NTFS ファイルシステムの暗号化、または圧縮されたファイルは InfoCage モバイル防御では暗号化できないため、NTFS ファイルシステムの暗号化、または圧縮している場合は、InfoCage モバイル防御をインストールする前に解除してください。
- 仮想ドライブの割り当ては行わないでください。
  (SUBST コマンドおよび MOUNTVOL コマンドを使用、または[コンピュータの管理]－[ディスクの管理]でドライブ文字またはパスの変更より[次の空の NTFS フォルダにマウントする]を使用など)
- InfoCage モバイル防御をインストール後は、コントロールパネル等からユーザのログオンやログオフの方法を変更することができなくなります。セキュリティ強化のため、[Ctrl+Alt+Del]キーを押下する画面を表示するように設定を変更する場合は、インストール前に設定変更してください。

● インストール後の注意事項

- スーパーバイザパスワード／ユーザパスワードは、InfoCage モバイル防御 ユーティリティの起動時、鍵の復旧時、アンインストール時に必要になりますので、絶対に忘れないように注意してください。
- InfoCage モバイル防御を正常にインストールした後に同じバージョンの setup.exe を実行すると、アンインストールのウィザードが起動しますので実行しないでください。
- Windows XP／2000 の場合、InfoCage モバイル防御の管理者の設定によっては、InfoCage モバイル防御をインストール後、Windows のセーフモードでの起動ができなくなる場合があります。
- Windows XP に InfoCage モバイル防御をインストールすると、OS 標準のバックアップ機能が使用できなくなります。バックアップを行う場合は、InfoCage モバイル防御のインストールフォルダ(通常は ¥Program Files¥NEC¥InfoCageCE)内の ¥tools¥MPBackup.exe を使用してバックアップを行ってください。操作方法については、「InfoCage モバイル防御 ユーザーズガイド」の「バックアップツールの利用」の項を参照してください。
- Windows XP に InfoCage モバイル防御をインストールすると、ユーザ選択画面が表示されなくなり、[簡易ユーザ切り替え]ができなくなります。また、シャットダウン時の画面が[コンピュータの電源を切る](ボタン選択)画面から、[Windows のシャットダウン](プルダウンメニュー選択)画面に変更されます。また、[Windows へようこそ]画面が通常のログオン画面に変更されます。
- InfoCage モバイル防御インストール後は ファイルシステムの変更(FAT および FAT32 から NTFS へのコンバート)は行えません。コンバートを行う場合は、いったん InfoCage モバイル防御をアンインストールしてから行ってください。
- InfoCage モバイル防御インストール後は、OS の再インストールおよびリカバリ、または内蔵ハードディスクのフォーマットは行わないでください。これらを行う場合は、いったん InfoCage モバイル防御をアンインストールしてから行ってください。
- Windows XP／2000 に InfoCage モバイル防御をインストールすると、OS 標準の[システムの復元]が使用できなくなります。
- Windows Vista 標準の[バックアップと復元センター]でバックアップを行う場合は、ファイルとフォルダのバックアップのみ行ってください。[Windows Complete PC バックアップ]は復元前と復元後で鍵やユーザパスワードが異なると、Windows へのログオンやファイルの参照ができなくなりますので使用しないでください。

● 暗号化について

・ 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。アプリケーションが使用しているファイルは、暗号化できない場合があります。

・ 暗号化や暗号化解除(復号)を行う場合、暗号化/復号処理の途中で、強制終了、Windows のロック、スクリーンセーバの設定の変更を行うとファイルが不正になりますので、絶対に行わないでください。

・ 以下の操作を行うとデータを正しく参照できなくなりますので、絶対に行わないでください。OS にログオンできなくなった場合などでデータを退避させたい場合でも、何も操作を行わず速やかに InfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したハードディスクを別のパソコンに接続し、データを移動する
  * セーフモードで起動し、暗号化したハードディスクから別のドライブにデータを移動する
  * Windows Vista 用の InfoCage モバイル防御 ユーティリティで暗号化したハードディスクドライブを、Windows XP/2000 用の InfoCage モバイル防御をインストールしたパソコンに装着する。またはその逆を行う。

・ NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントの変更権限が必要です。

参照 SYSTEMアカウントの変更方法は、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。

・ NTFS ファイルシステムで暗号化または圧縮されたファイルは暗号化できません。

・ 暗号化指定したフォルダを共有設定しないでください。

・ 旧バージョンの InfoCage モバイル防御で暗号化した外部メディアおよびハードディスクドライブを本バージョンの InfoCage モバイル防御がインストールされているパソコンに装着した場合、一部のファイルが正常に読み込みできないことがあります。

・ 万が一、使用中に次のような現象が発生した場合は、大切なデータを損失する可能性がありますので、現象が発生した状態のまま何も操作を行わず、速やかに InfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したはずのファイルが読み書きできない(文字化けなど)
  * OS にログオンできない
  * 作成した鍵が使用できない(メディア鍵認証方式の場合)

● アップグレードインストールの注意事項

・ アップグレードインストールを行う場合、すでにインストール済みの InfoCage モバイル防御をアンインストールする必要はありません。

・ 暗号化した外付けハードディスクドライブおよびリムーバブルディスクがある場合は、必ずパソコンに装着した状態でアップグレードインストールを行ってください。パソコンから取り外した状態でアップグレードした場合、一部のファイルが正常に読み込みできないことがあります。

・ お使いのバージョンによってはアップグレードインストールの途中で数回再起動を行う場合があります。メッセージにしたがって操作してください。

・ 外部メディア自動暗号機能や FeliCa カードでの認証機能については、セットアッププログラムのカスタマイズを行い、アップグレードインストールすることで、各機能が有効になります。カスタマイズ方法については、「InfoCage モバイル防御 管理者ガイド」を参照してください。

・ バージョンにかかわらずアップグレードインストール後も設定を引き継ぐものは以下の通りです。

  * スーパーバイザパスワード/ユーザパスワード
  * 鍵および鍵情報(InfoCage モバイル防御 Ver1.0 で鍵情報をネットワーク共有フォルダに作成している場合もそのまま引き継がれます。)
  * 暗号化指定されたドライブ/フォルダ
  * 管理サーバでの設定内容(ネットワークモードで運用している場合)
  * インストール先のフォルダ

* クライアント初期設定ツールでセットアッププログラムをカスタマイズしてインストールした設定内容
* その他のユーティリティでの設定内容
(InfoCage モバイル防御ユーティリティおよびメディア暗号ユーティリティ)

・ Ver3.5 より以前のバージョンからアップグレードインストールを行った場合に変わるものは以下の通りです。

* プログラム名
[MobileProtect]
↓
[InfoCage モバイル防御]

* スタートメニューからの起動方法
[すべてのプログラム]-[MobileProtect]
↓
[すべてのプログラム]-[NEC]-[InfoCage モバイル防御]

* ユーザーズガイド
[MobileProtect オンラインマニュアル]
↓
[InfoCage モバイル防御 ユーザーズガイド]

● メディア鍵認証方式の注意事項

・ 事前に準備していただくもの
インストールには外部メディアが 2 個必要です。
ご使用にあたっては、鍵を作成するメディア(*1)と、鍵情報を作成するためのメディア(*2)が必要です。
各メディアはインストール前にフォーマットしておいてください。

Notice
メディアをフォーマットせずに使用した場合、鍵の作成や復旧ができない場合があります。

*1:鍵は、USB メモリ、フラッシュメモリカード、フロッピーディスク (Windows XP/2000 の場合のみ)、モバイルディスク等の他、サーバの共有フォルダに作成できます。(推奨:USB メモリ)
*2:フロッピーディスク、USB メモリ、フラッシュメモリカード、モバイルディスク等が使用できます。

・ 注意事項

(1) 鍵について
InfoCage モバイル防御で保護されたパソコンを使用する際には、必ず鍵を作成したメディアを装着した状態で使用してください。

(2) 鍵情報について
・「鍵情報」を紛失すると「鍵」の復旧ができませんので、「鍵情報」を保存したメディア内のデータを絶対に紛失しないように注意してください。
・ スタンドアローン運用時、鍵情報は鍵を作成したメディアには保存できません。

● パスワード認証方式の注意事項

・ セキュリティチップ (TPM) を使用している場合、以下の操作を行うと、暗号化されたファイルにアクセスできなくなりますので絶対に行わないでください。これらを行う場合は、いったん InfoCage モバイル防御をアンインストールしてから行ってください。
* セキュリティチップ (TPM) は Windows XP でパスワード認証方式を導入する場合のみ使用可能です。

* BIOS でセキュリティチップを[使用しない]に設定を変更する
* BIOS のアップデートなどで設定値を初期化する
* セキュリティチップユーティリティをアンインストールする

● ハードウェア／アプリケーション競合問題について

次のハードウェアおよびアプリケーションソフトは、InfoCage モバイル防御と同時に利用、または InfoCage モバイル防御がインストールされた環境で利用すると、問題が発生することがあります。
これらは InfoCage モバイル防御をインストールする前にアンインストール、または取り外しておいてください。
アプリケーションをアンインストールできない場合は使用しないでください。

⚠Notice

- 下記はこれまで報告のあったハードウェアおよびアプリケーションソフトの一覧を記載しております。記載のないハードウェアおよびアプリケーションソフトの動作を保証するものではありません。(2008 年 1 月現在)
- 最新情報は以下に掲載しております。
  http://www.nec.co.jp/cced/infocage/m_defense/env.html

InfoCage モバイル防御と共存できないハードウェア／アプリケーション

× ・・・共存できないことを確認済みのハードウェア／アプリケーション

空欄 ・・・OS 未対応または未確認のハードウェア／アプリケーション

ハードウェア／アプリケーションの種類	Windows Vista	Windows XP/2000
・ハードウェア		
I/O データ UIDE-133R2(RAID ボード)		×
・他のファイル暗号化ソフト、一部の独自のログオン認証を行うソフト、BitLocker ドライブ暗号化(Windows Vista の統合セキュリティ機能)	×	×
・Pointsec Media Encryption		×
・仮想マシン環境構築ソフト(Microsoft VirtualPC など)	×	×
・データバックアップ、リカバリソフト		
(PowerX StandbyDisk4、FINALDATA2007、Acronis True Image LE、Acronis True Image 10 など)	×	
(StandbyDisk、StandbyDisk Solo、StandbyDisk Solo RB、FINALDATA、Acronis True Image LE、Acronis True Image 8.0 など)		×
・一部のディスクイメージ(HDD バックアップ)作成ソフト(V2i Protector など)		×
・ティアック株式会社 Swipe FINGERPRINT USB メモリ および NEC 製ノートパソコン内蔵の指紋センサ以外を使用する指紋認証システム (NEC 製ノートパソコン内蔵の指紋センサを使用した認証システムと、InfoCage モバイル防御の認証システムとの併用が可能です。ただし、Swipe FINGERPRINT USB メモリのように連携させることはできません。)		×
・一部のライティングソフト(B's CLiP など)		×
・一部の PC プレインストールソフト		
(IBM/レノボ製 PC に付属のバックアップソフト「Rapid Restore Ultra/Rescue and Recovery」	×	×
松下電器製 PC に搭載されている「オプティカルディスク省電力ユーティリティ」 など)		×
・McAfee プライバシーサービス		×
・Acronis True Image LE、True Image 8.0		×
・Acronis DriveCleanser		×

ハードウェア／アプリケーションの種類	Windows Vista	Windows XP/2000
・ DiskXtender		×
・ PartitionMagic		×
・ Windows ReadyBoost	×	
・一部のウイルス対策ソフト （GRISOFT AVG Anti-Virus、eTrust Antivirus、McAfee Managed Total Protection 4.x（4.0.0.395 以降）、Eset NOD32 など）		×
・ Google パック(Norton SecurityScan Ver.1.1.0.27）		×
・Norton SystemWorks（Norton Utilities）の Norton Protection（ごみ箱機能） 使用している場合は InfoCage モバイル防御をインストールする前に解除してください。 ＜解除方法＞ 1.デスクトップの[Norton ごみ箱]のアイコンを右クリックし、[プロパティ]をクリックしてください。 2.[Norton Protection]タブを選択してください。 3.プルダウンメニュー[ドライブ]で、ドライブを選択し、[保護を有効にする]チェックを外してください。 ※必ず全ドライブ無効にしてください。 4.[OK]をクリックしてください。 ※ 設定を変更しない場合、ファイルの暗号化や復号に失敗する可能性があります。		×

使用に制限のあるハードウェア／アプリケーション（Windows XP／2000）

ハードウェア／アプリケーションの種類	対策
ハードウェア	
SOTEC Winbook WV730（PC 本体）	BIOS をアップグレードすることにより利用可能 （Ver は 1.03ST → 1.05ST）
独自のセキュリティ機能を持つ USB メモリ （IO Data　EasyDisk for Security など）	鍵以外では利用可能。（鍵メディアとして利用不可）
CD-R 等ライティングソフト　(*)	
・Windows XP 標準の CD 書き込み機能	ファイルを書き込みする場合は、暗号化されていないフォルダにファイルをコピーもしくは移動した後に操作を行うことで利用可能
・DirectCD	
ウイルス対策ソフト	
・SymantecAntiVirusCorprateEdition10.0 （MR2 MP2 より以前のバージョン）	パッチ適用により利用可能
・Symantec Client Security 3.0.2 （MR2 MP2 より以前のバージョン）	
・Norton AntiVirus2006	
その他ソフト	
・Symantec pcAnywhere	・pcAnywhere→モバイル防御の順でインストールすることで利用可能 ・モバイル防御→pcAnywhere の順でインストールする際は、パッチ適用で利用可能
・Pointsec	・ディスク暗号による暗号化環境での利用不可。
・NETWIZARD	・[ReachOut サービスを停止しました]エラーを閉じてログオンすることで利用可能。閉じずにログオンした場合は Ctrl+Alt+Del を押下してエラーを再表示し閉じることにより利用可能。

ハードウェア／アプリケーションの種類	対策
	・閉じずにログオンした場合は Ctrl+Alt+Del を押下してエラーを再表示し閉じることにより利用可能。
・BIGLOBE リモートアクセスサービス VPN クライアント	・VPN ソフト→モバイル防御の順番でインストールすることで利用可能
・ローミングクライアント	以下のどちらかで利用可能 ・ローミングクライアント→モバイル防御の順でインストール。 ・ローミングクライアントのレジストリを編集。 ただし、ドメイン環境使用時には上記回避策のみではドメインログオンができなくなります。モバイル防御の初期設定ファイルを置換することで利用可能。
・WebSAM WinShare	・WebSAM WinShare→モバイル防御の順でインストールすることで利用可能。
・Socia 給与システム	以下のどちらかで利用可能。 ・Oracle9.2i 以上を利用する。 ・Oracle インストールフォルダ（データベース格納フォルダ含む）を暗号化対象外とすることで回避可能。
・InfoCage 持ち出し制御 クライアント	以下の手順で利用可能 (1)InfoCage 持ち出し制御をアンインストールする。 (2)InfoCage モバイル防御をインストールし、再起動後に暗号化を行う。 (3)InfoCage 持ち出し制御 クライアントをインストールする。
・4thEye Professional++ クライアント版	※ 4hEye との共存については、別途お問い合わせください。

(*) 下記のライティングソフトは InfoCage モバイル防御とは併用が可能であることを確認しています。

- RecordNow
- B’s Recorder Gold
- Easy CD Creator

2.3　【導入前の注意事項】確認チェックシート

InfoCage モバイル防御をインストールする前に、以下の項目をチェックしてください。

	確 認 事 項	チェック欄	
		メディア鍵 認証方式	パスワード 認証方式
1	重要なデータは、念のためバックアップを取ること。		
2	鍵用のメディア、あるいはサーバを用意すること。		／
3	十分な空き容量が各ドライブにあること。 ※暗号化を実行する際、テンポラリ（一時作業スペース）として以下の空き容量がドライブごとに必要になります。 必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋ （ドライブ容量×0.02） （上記は最低限必要な容量です。暗号化処理は、十分な空き容量がある状態で行ってください。） ※ただし、初めて暗号化処理を行う場合はすべてのドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。		
4	共存不可のアプリケーションの確認・対策を行うこと。 ※「アプリケーション競合問題について」を参照		
5	暗号化するフォルダやファイルに SYSTEM アカウントの変更権限があることを確認すること。		
6	デュアルブートマシンでないこと。		
7	仮想ドライブを割り当てていないこと。		

第3章 インストール

InfoCage モバイル防御のインストールを行います。

⚠Notice

アップグレードインストールを行う場合は、「第 5 章 アップグレードインストール」を参照してください。

3.1 インストールの前に

■ 確認事項

インストールの前に次のことを確認してください。

□ 注意事項はすべて確認しましたか？

注意事項は「2.2注意事項」を参照してください。

□ 「【導入前の注意事項】確認チェックシート」を実施しましたか？

確認チェックシートは「2.3【導入前の注意事項】確認チェックシート」を参照してください。

□必要なものは揃っていますか？

InfoCage モバイル防御の管理者から次のものが配布または通知されているか確認してください。

運用方法の通知（メディア鍵認証方式またはパスワード認証方式） ※
プロダクト ID の通知
鍵および鍵情報を保存するメディアの配布（メディア鍵認証方式の場合）
暗号化するドライブ／フォルダの通知（個別暗号モードインストールの場合） ※
許可外部メディアの配布（許可外部メディアを利用する場合）

（※） InfoCage モバイル防御の管理者より、あらかじめセットアッププログラムに設定されている場合があります。

3.2 パソコンの環境チェック

インストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。

3.2.1 環境チェックユーティリティ

■ Windows Vista の場合

1. InfoCage モバイル防御が格納されているメディア（例 CD-ROM）内の¥Vista¥Tools¥環境チェック UTL ¥MPEnvChk.exe を実行してください。

> **Notice**
> CD-ROM からコピーして使用する場合は、環境チェック UTL フォルダをデスクトップなどにコピーしてから実行してください。（MPEnvChk.exe は実行ファイルのみをコピーしても動作しません。）

2. 環境チェックユーティリティの説明が表示されます。
[OK]をクリックして、起動しているアプリケーションや常駐プログラムを必ず終了してください。

3. [ドライブ]に表示されているドライブのうち、暗号化するドライブにチェックを入れ、[開始]をクリックしてください。

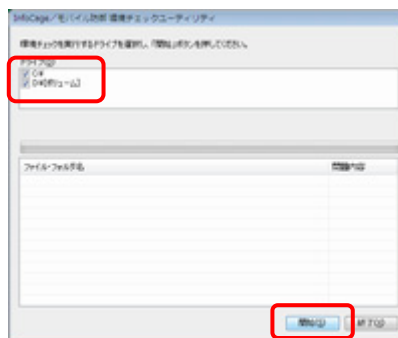
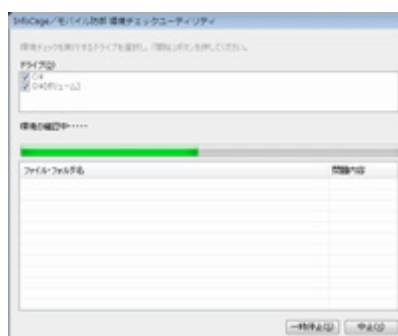
4. 環境をチェックしています。しばらくお待ちください。

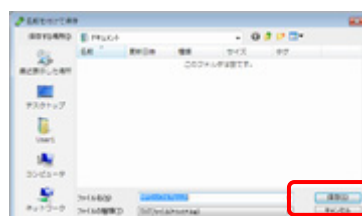
5. 問題が見つかった場合は、[ファイル・フォルダ名]に表示されているファイルを選択し、[対処方法]をクリックします。

6. 対処方法が表示されます。内容を確認し、[閉じる]をクリックします。

参照 アクセス権に関する対象方法については、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。

7. ファイルを選択している状態で[開く]をクリックすると、ファイルのあるフォルダが開きます。
対処方法に表示されていた内容にしたがって、対処してください。

8. 環境チェックユーティリティを終了する場合は、[終了]をクリックします。

9. 問題の一覧を保存する場合は[はい]をクリックします。

10. 保存する場所を指定し、[保存]をクリックします。

11. ファイルに出力しました。[OK]をクリックします。

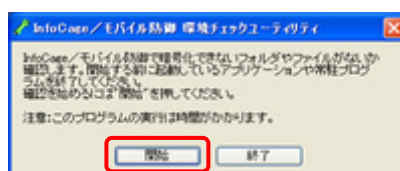
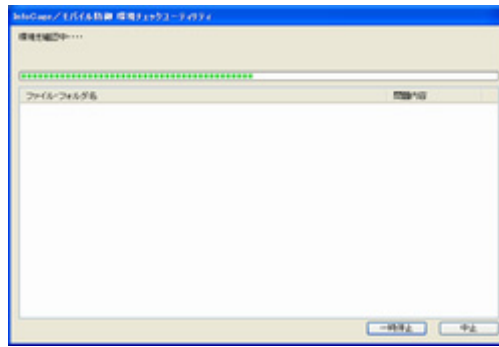
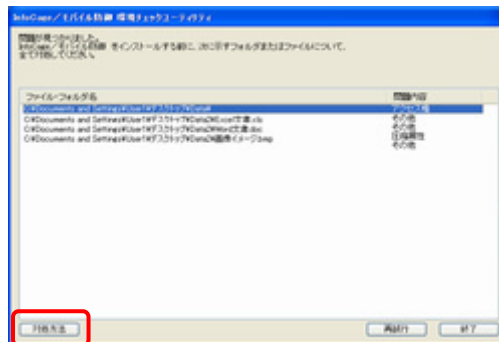
以上で環境チェックは完了です。

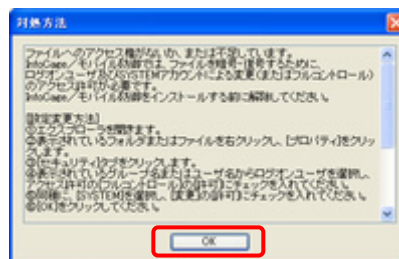
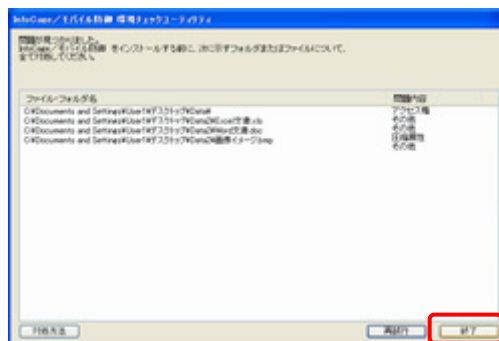
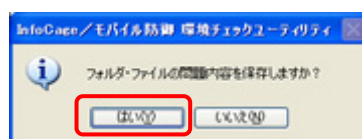
見つかった問題の対処が完了したら、InfoCage モバイル防御をインストールします。

■ Windows XP／2000 の場合

1. InfoCage モバイル防御が格納されているメディア(例 CD-ROM)内の¥2K_XP¥Tools¥環境チェック UTL ¥MPEnvChk.exe を実行してください。
アップグレードインストールを行う場合は、¥2K_XP¥Tools¥環境チェック UPG¥MPEnvChkUpg.exe を実行してください。

> **⚠Notice**
> CD-ROM からコピーして使用する場合は、環境チェック UTL フォルダをデスクトップなどにコピーしてから実行してください。(MPEnvChk.exe は実行ファイルのみをコピーしても動作しません。)

2. 環境チェックユーティリティの説明が表示されます。
起動しているアプリケーションや常駐プログラムを必ず終了し、[開始]をクリックしてください。

3. 環境をチェックしています。しばらくお待ちください。

4. 問題が見つかった場合は、[ファイル・フォルダ名] に表示されているファイルを選択し、[対処方法] をクリックします。

5. 対処方法が表示されます。内容を確認し、[OK]をクリックします。

参照 アクセス権に関する対象方法については、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。

6. 環境チェックユーティリティを終了する場合は、[終了]をクリックします。

7. 問題の一覧を保存する場合は[はい]をクリックします。

8. 保存する場所を指定し、ファイル名を入力して[保存]をクリックすると問題の一覧ファイルが保存されます。

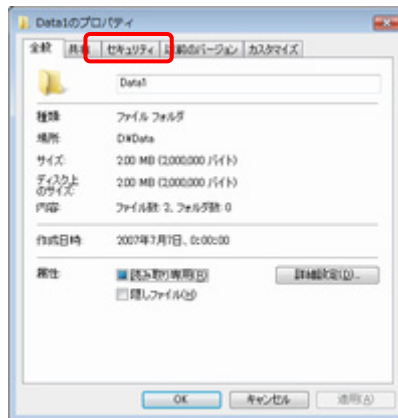
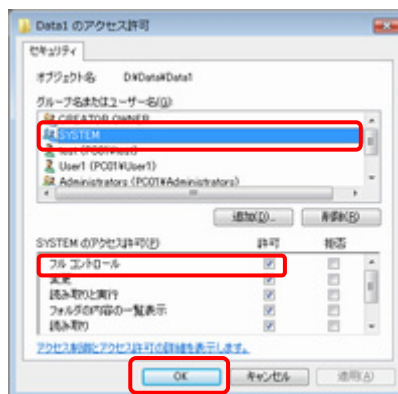
以上で環境チェックは完了です。

見つかった問題の対処が完了したら、InfoCage モバイル防御をインストールします。

3.2.2 SYSTEM アカウントの変更方法

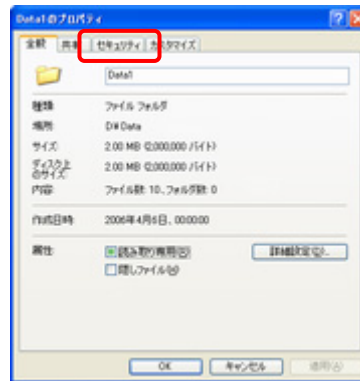
NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントのフルコントロール権限または変更権限が必要です。
(Windows Vista および Windows XP Professional 、Windows 2000 のみ変更可能です。)
ここでは D:¥Data¥Data1 フォルダの SYSTEM アカウントを変更する方法を説明します。

■ Windows Vista の場合

1. SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から[プロパティ]をクリックしてください。フォルダのプロパティ画面が表示されます。

2. [セキュリティ]タブを選択し、[編集]をクリックしてください。アクセス許可の編集画面が表示されます。
[グループ名またはユーザ名]から[SYSTEM]を選択し、[アクセス許可]の[フルコントロール]の[許可]にチェックを入れ、[OK]をクリックしてください。
これで SYSTEM アカウントが変更されました。[OK]をクリックして画面を閉じます。

⚠Notice

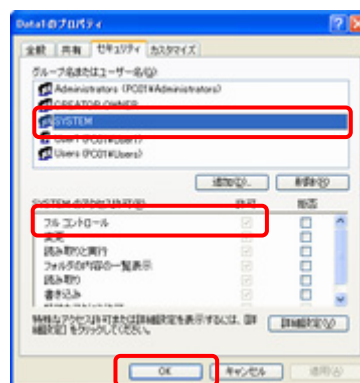
[グループ名またはユーザ名]内に[SYSTEM]が表示されていない場合は、次の方法で表示させてください。
1. [グループ名またはユーザ名]の下の[編集]をクリックし、[アクセス許可]の画面で[追加]をクリックします。
2. 表示された画面の[選択するオブジェクト名を入力してください]に[SYSTEM]と入力し、[名前の確認]をクリックします。
3. [選択するオブジェクト名を入力してください]に[SYSTEM]と表示されますので、[OK]をクリックします。

■ Windows XP／2000 の場合

1. SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から[プロパティ]をクリックしてください。フォルダのプロパティ画面が表示されます。

⚠ Notice

[セキュリティ]タブが表示されていない場合は、次の方法で表示させてください。

1. SYSTEM アカウントを変更したいフォルダを開きます。
2. [ツール]－[フォルダオプション]－[表示]－[簡易ファイルの共有を使用する]のチェックを外して、[OK]をクリックしてください。

2. [セキュリティ]タブを選択してください。
[グループ名またはユーザ名]から[SYSTEM]を選択し、[アクセス許可]の[フルコントロール]の[許可]にチェックを入れ、[OK]をクリックしてください。
これで SYSTEM アカウントが変更されました。

⚠ Notice

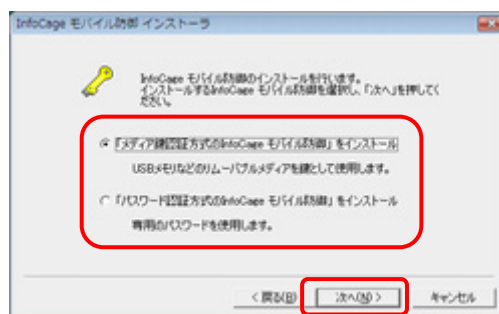
[グループ名またはユーザ名]内に[SYSTEM]が表示されていない場合は、次の方法で表示させてください。

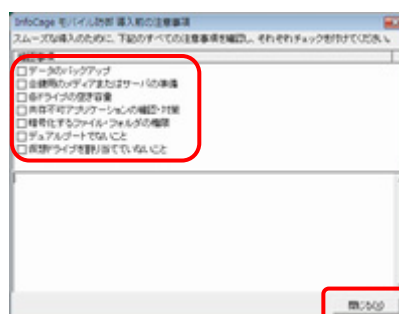
1. [グループ名またはユーザ名]の下の[追加]をクリックします。
2. 表示された[ユーザまたはグループの選択]画面の[選択するオブジェクト名を入力してください]に[SYSTEM]と入力し、[名前の確認]をクリックします。
3. [選択するオブジェクト名を入力してください]に[SYSTEM]と表示されますので、[OK]をクリックします。

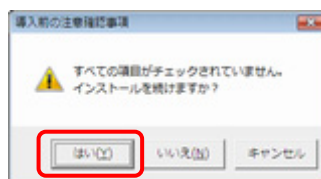
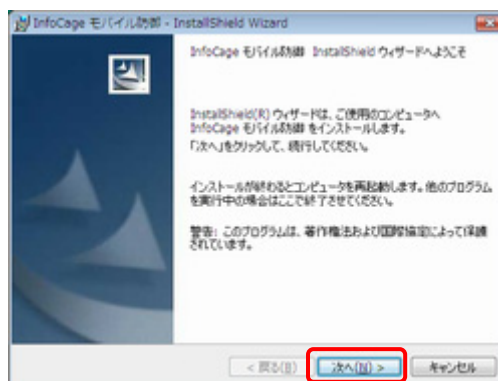
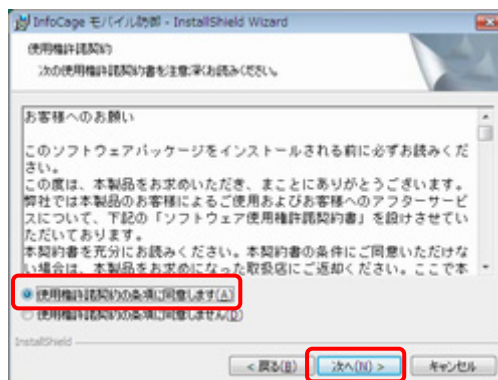
3.3　Step1

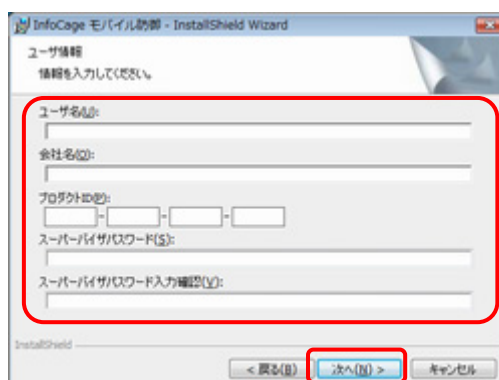
InfoCage　モバイル防御をインストールします。下記の手順で操作してください。

1. InfoCage　モバイル防御が格納されているメディア（例　CD-ROM）内の setup.exe を実行し、［次へ］をクリックしてください。

2. ［「メディア鍵認証方式の　InfoCage　モバイル防御」をインストール］または［「パスワード認証方式の　InfoCage　モバイル防御」をインストール］のいずれかを選択し、［次へ］をクリックしてください。

Notice
InfoCage　モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。

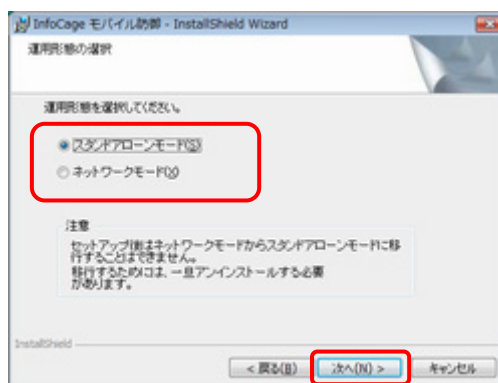
3. ［導入前の注意事項］　画面が表示されます。
各項目をクリックすると詳細な説明が表示されますので、必ずすべての注意事項を確認し、チェックを付けてください。
すべての確認が終わりましたら、［閉じる］をクリックしてください。

Notice
画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部異なります。

4. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は[はい]をクリックしてください。
インストールを中止する場合は[いいえ]を、*3* の画面に戻る場合は[キャンセル]をクリックしてください。

5. [次へ]をクリックしてください。

6. 使用権許諾契約をすべて確認し、同意する場合は[使用権許諾の条項に同意します]を選択し、[次へ]をクリックしてください。
[使用権許諾の条項に同意しません]を選択した場合はインストールできません。

7. ユーザ情報を入力します。

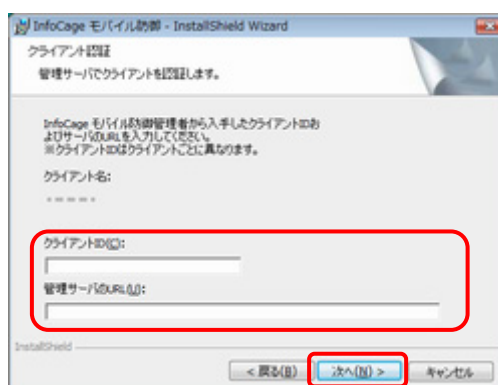
ユーザ名、会社名、プロダクト ID、スーパーバイザパスワード／ユーザパスワードを入力します。
（確認のため、スーパーバイザパスワード／ユーザパスワードは 2 回入力してください。）
すべての入力が終わりましたら、[次へ]をクリックしてください。

ユーザ名、会社名	半角 40 文字以内、または全角 20 文字以内で入力してください。
プロダクト ID	ライセンス証書に記載されているものを半角文字で入力してください。 （大文字小文字は区別しません）。
スーパーバイザパスワード	8 文字以上 64 文字以内の半角英数および記号を指定してください。 （大文字小文字を区別します）。
ユーザパスワード	8 文字以上 32 文字以内の半角英数および記号を指定してください。 （大文字小文字を区別します）

Notice

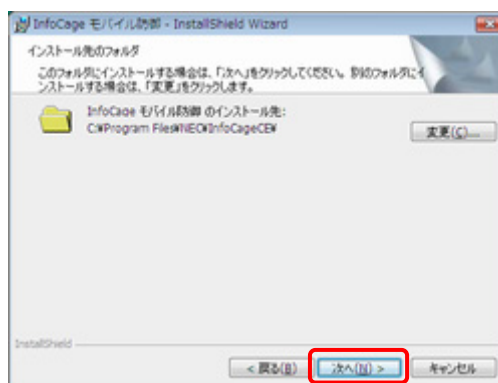
- 画面はメディア鍵認証方式版のものです。パスワード認証方式版の場合は、[スーパーバイザパスワード]の欄は[ユーザパスワード]と表示されます。
- スーパーバイザパスワード／ユーザパスワードとは InfoCage モバイル防御ユーティリティを起動するときなどに必要なパスワードです。忘れないよう注意してください。

8. ［運用形態の選択］ 画面で、運用形態の選択をします。
［スタンドアローンモード］または［ネットワークモード］を選択し、［次へ］をクリックしてください。

⚠Notice

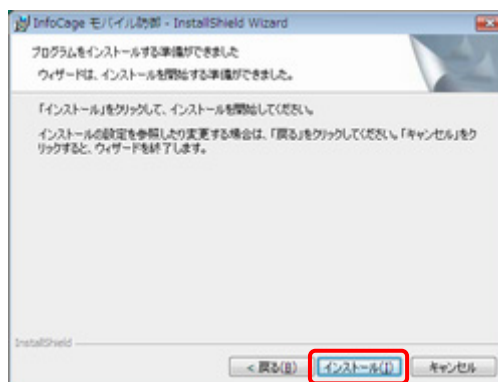
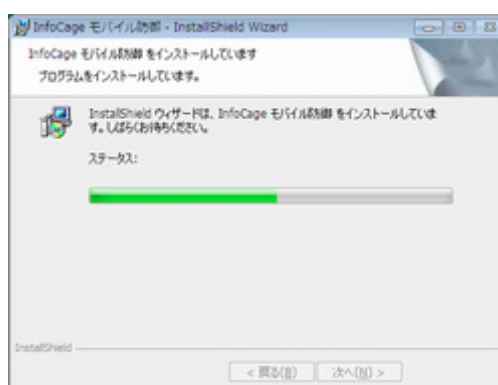
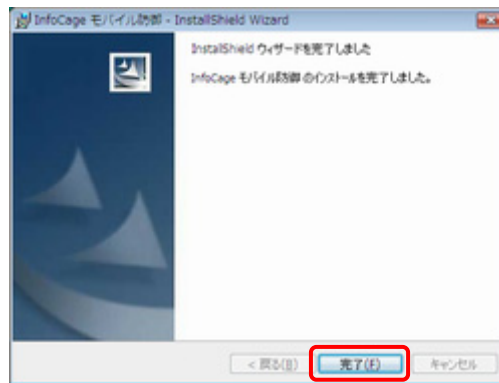
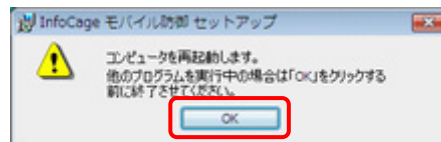
- 別売の InfoCage モバイル防御 管理サーバが導入されていない環境では、スタンドアローンモードを選択してください。
  また、InfoCage モバイル防御管理サーバが導入されている環境では、InfoCage モバイル防御の管理者に問い合わせて運用形態を選択してください。
- InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。
- スタンドアローンモードを選択した場合は *10* へ進んでください。

9. *8* でネットワークモードを選択した場合、クライアント認証画面が表示されます。
クライアントID、管理サーバのURLを入力して、［次へ］をクリックしてください。

⚠Notice

- スタンドアローンモードの場合、この画面は表示されません。
- 認証に失敗した場合は、クライアント名、クライアント ID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。
- InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。
- その他の理由で認証に失敗した場合は、以下を参照してください。
  参照 第 11 章 トラブルシューティング (2)

10. インストール先のフォルダ選択画面で InfoCage モバイル防御のインストールフォルダを選択します。
通常はそのまま[次へ]をクリックしてください。

⚠ Notice

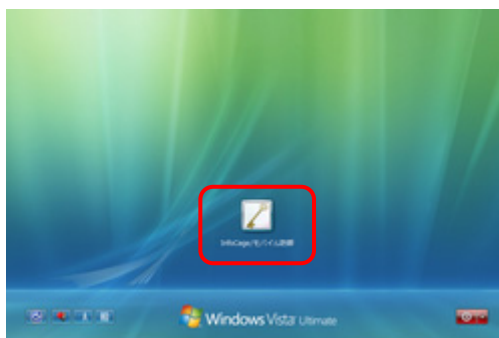
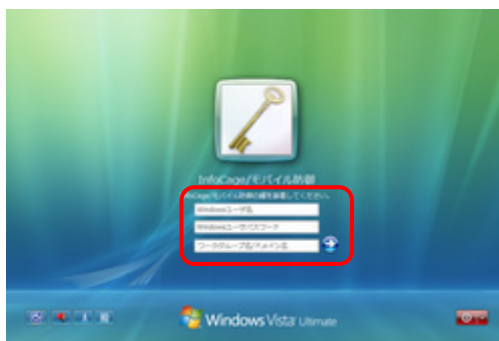
日本語または英語以外の文字を含むフォルダにインストールすることはできません。

11. [インストール]をクリックしてインストールを開始してください。

12. インストール中です。しばらくお待ちください。

13. インストールが完了すると下記の画面が表示されます。
［完了］をクリックしてください。

14. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。
他のプログラムを実行中の場合は、終了させてください。
［OK］をクリックすると、パソコンが再起動します。

再起動後の操作は、次章以降を参照してください。

3.4 Windows へログオン

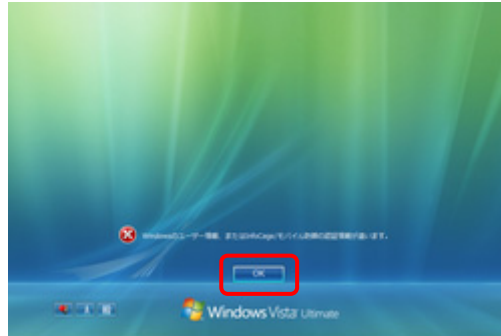
InfoCage モバイル防御をインストールすると、Windows のログオン方法が変わります。
再起動後は以下の手順で Windows へログオンします。

■ Windows Vista の場合

1. InfoCage モバイル防御のボタンをクリックします。

2. Windows のユーザ名およびパスワードを入力し、 をクリックするか Enter キーを押すと、Windows へログオンすることができます。
パスワード認証方式の場合は[InfoCage モバイル防御 パスワード]に、インストール時に設定したユーザパスワードを入力してください。

Notice

- 画面はメディア鍵認証方式のものです。
- ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。
(ワークグループの場合は空欄でも可。)

●ユーザ情報エラーの場合

メディア鍵認証方式の場合は鍵を抜いた状態、パスワード認証方式の場合は誤ったユーザパスワードでログオンしようとすると、［Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。］ と表示され、Windows へログオンできません。
［OK］をクリックして、*2* に戻って操作してください。

■ Windows XP／2000 の場合

● メディア鍵認証方式の場合

1. 再起動後に［Windows へようこそ］画面が表示されます。
Ctrl＋Alt＋Del キーを押してください。

> **Notice**
> Windows の設定によっては、［Windows　へようこそ］画面は表示されません。

2. ［Windows へログオン］画面が表示されます。
正しいパスワードを入力して［OK］をクリックすると Windows へログオンすることができます。

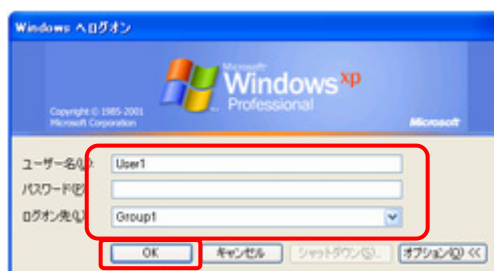
● パスワード認証方式の場合

1. 再起動後に[Windows へようこそ]画面が表示されます。
Ctrl＋Alt＋Del キーを押してください。

Notice
Windows の設定によっては、[Windows へようこそ]画面は表示されません。

2. ユーザパスワード入力画面が表示されます。
インストール時に設定したユーザパスワードを入力し、[OK]をクリックしてください。

Notice
ユーザパスワードを 5 回連続で誤って入力すると、[OK]がクリックできなくなります。
その場合は[シャットダウン]をクリックしていったんシャットダウンした後、再度パソコンを起動してパスワード入力画面が有効になるまでしばらくお待ちください。
（すぐにパソコンを起動しても一定時間パスワードの入力はできません。）

3. [Windows へログオン]画面が表示されます。
正しいパスワードを入力して[OK]をクリックすると Windows へログオンすることができます。

続いて次章「3.5 Step」へ進み、それぞれの認証方式の項を参照してください。

3.5.1 メディア鍵認証方式の場合

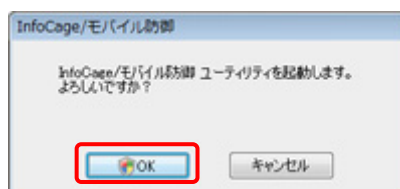
3.5.2 パスワード認証方式の場合

InfoCage モバイル防御の管理者の設定により、個別暗号モードでインストールした場合は、「第 4 章 個別暗号モードインストール」へ進んでください。

3.5 Step2

再起動後、暗号化ウィザードが起動します。
それぞれの認証方式の説明にしたがって、暗号化を行ってください。

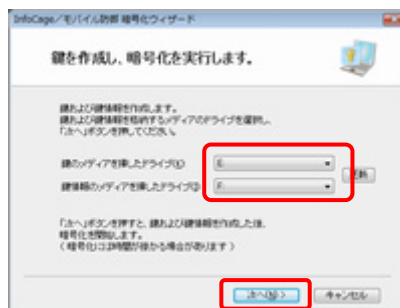
> ⚠ Notice
>
> 何らかの理由で暗号化ウィザードを終了した場合、再度暗号化ウィザードを起動するには、スタートメニューから［すべてのプログラム］－［NEC］－［InfoCage モバイル防御］－［InfoCage モバイル防御 ユーティリティ］をクリックします。

3.5.1 メディア鍵認証方式の場合

1. Windows Vista の場合は再起動後に、以下の画面が表示されます。
［OK］をクリックしてください。

> ⚠ Notice
>
> ［キャンセル］をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを起動して、パソコンの鍵を作成および暗号化を行ってください。

2. 鍵を格納するメディアと鍵情報を格納するメディアを装着し、インストール時に設定したスーパーバイザパスワードを入力して［次へ］をクリックしてください。

> ⚠ Notice
>
> 他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した外部メディアは、暗号化を実行する前に必ず抜いてください。
> 装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん［キャンセル］をクリックし、外部メディアを抜いてから再度暗号化ウィザードを起動してください。

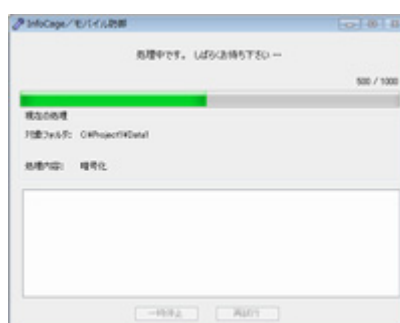
3. 鍵および鍵情報を作成します。
鍵を格納するメディア および 鍵情報を格納するメディアのドライブを選択してください。
格納するメディアが表示されないときは、[更新]をクリックします。
[次へ]をクリックしてください。

⚠Notice

- ネットワークモードの場合や InfoCage モバイル防御の管理者によりあらかじめ鍵および鍵情報の格納先が設定されている場合は上記の画面が一部異なります。
- ここではネットワークの共有フォルダに鍵を作成することはできません。共有フォルダに鍵を作成する場合はいったん外部メディアに鍵を作成し、暗号化終了後に合鍵として作成してください。
- ネットワークモードの場合で管理サーバと通信できないときは、以下を参照してください。
  参照 第 11 章 トラブルシューティング (2)

4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。
[はい]をクリックすると暗号化が開始されます。

⚠Notice

- アプリケーションが使用しているファイルは、暗号化できない場合があります。
- 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
  またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

5. 暗号化処理中です。しばらくお待ちください。

6. 暗号化を完了しました。
[完了]をクリックしてください。

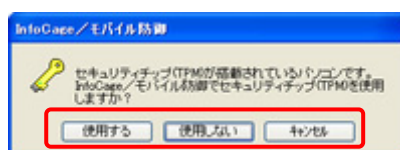
以上で暗号化は完了しました。
その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

Notice

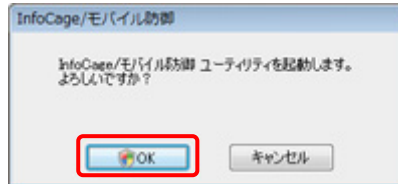
この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。
Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。(Windows XP／2000 のみ)

3.5.2 パスワード認証方式の場合

● **セキュリティチップ(TPM)搭載のパソコンをお使いでセキュリティチップ(TPM)が有効になっている場合**

Windows XP の場合、InfoCage モバイル防御の管理者の設定によっては、再起動後にユーザパスワードを入力して Windows にログオンすると、下記の画面が表示される場合があります。

セキュリティチップ(TPM)を使用する場合は[使用する]を、使用しない場合は[使用しない]を、後で選択する場合は[キャンセル]をクリックしてください。
ただし、[キャンセル]をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御 ユーティリティの起動時にメッセージが表示されます。

セキュリティチップ(TPM)に関しては、「第 10 章 セキュリティチップ(TPM)搭載のパソコンをお使いの場合」を参照してください。

● ログオン認証にパスワードを使用する場合

1. Windows Vista の場合は再起動後に、以下の画面が表示されます。
[OK]をクリックしてください。

⚠Notice

［キャンセル］をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを起動して、パソコンの鍵を作成および暗号化を行ってください。

2. ユーザパスワードを入力して[次へ]をクリックしてください。

⚠Notice

他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した外部メディアは、暗号化を実行する前に必ず抜いてください。
装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん［キャンセル］をクリックし、外部メディアを抜いてから再度暗号化ウィザードを起動してください。

3. 暗号化を実行します。[次へ]をクリックしてください。

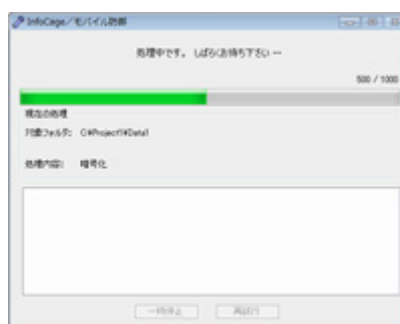
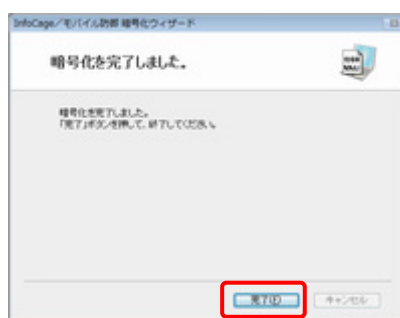
⚠Notice

暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。
[はい]をクリックすると暗号化が開始されます。

⚠Notice

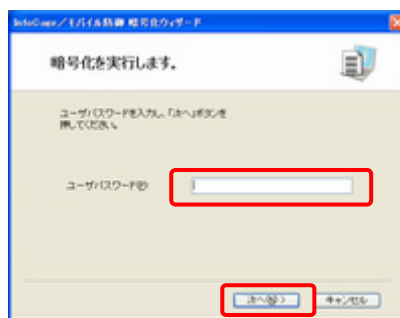
アプリケーションが使用しているファイルは、暗号化できない場合があります。
暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

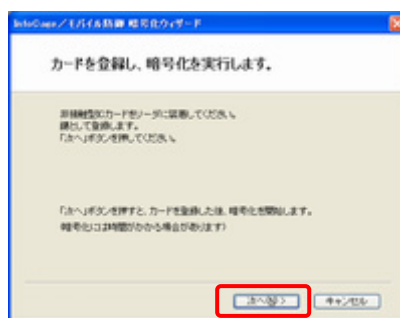
5. 暗号化処理中です。しばらくお待ちください。

6. 暗号化を完了しました。
[完了]をクリックしてください。

以上で暗号化は完了しました。
その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

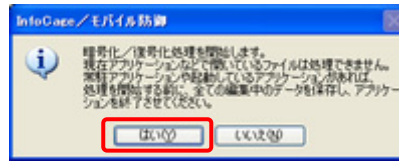
⚠Notice

この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。
Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。(Windows XP／2000 のみ)

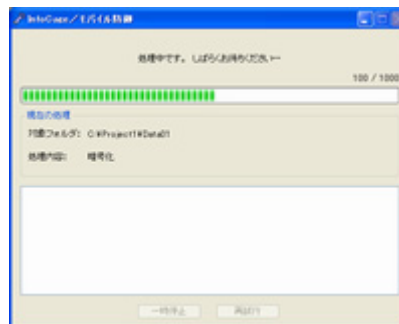
● ログオン認証に FeliCa カードを使用する場合 （Windows XP/2000 のみ）

1. インストール時に設定した InfoCage モバイル防御のユーザパスワードを入力して Windows にログオンすると、下記の画面が表示されます。
ユーザパスワードを入力して[次へ]をクリックしてください。

> **Notice**
>
> 他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した外部メディアは、暗号化を実行する前に必ず抜いてください。
> 装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん[キャンセル] をクリックし、外部メディアを抜いてから再度スタートメニューから[すべてのプログラム]－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ]をクリックし、暗号化ウィザードを起動して操作してください。

2. FeliCa カードをカードリーダにセットして[次へ]をクリックしてください。

> **Notice**
>
> FeliCa のカードリーダを使用可能な状態にしてから操作してください。

3. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。
［はい］をクリックすると暗号化が開始されます。

Notice

- アプリケーションが使用しているファイルは、暗号化できない場合があります。
- 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
  またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、ごみ箱を空にしておくことをお奨めします。

4. 暗号化処理中です。しばらくお待ちください。

5. 暗号化を完了しました。
［完了］をクリックしてください。

以上でインストールは完了しました。
その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

Notice

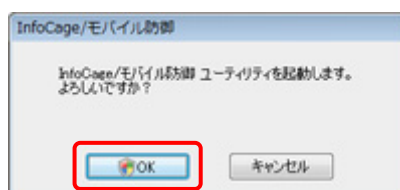
この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。
Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。（Windows XP／2000 のみ）

第4章　個別暗号モードインストール

InfoCage　モバイル防御は、インストール後の暗号化モード(ドライブ一括暗号モード　または　個別暗号モード)を InfoCage　モバイル防御の管理者により選択することができます。
「個別暗号モード」に設定されたセットアッププログラムを使用した場合、インストールを完了し再起動した後は、本章のそれぞれの認証方式の説明にしたがって操作してください。

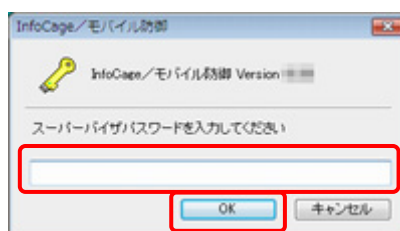
⚠Notice

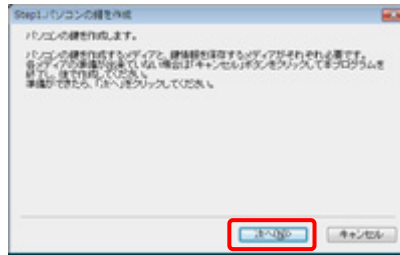
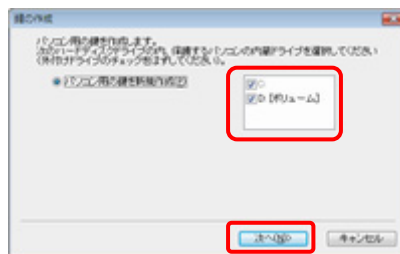
何らかの理由で暗号化ウィザートを終了した場合、再度暗号化ウィザードを起動するには、スタートメニューから［すべてのプログラム］－［NEC］－［InfoCage　モバイル防御］－［InfoCage　モバイル防御　ユーティリティ］をクリックします。

4.1　メディア鍵認証方式の場合

1. Windows Vista の場合は再起動後に、以下の画面が表示されます。
［OK］をクリックしてください。

⚠Notice

［キャンセル］をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを起動して、パソコンの鍵を作成および暗号化を行ってください。

2. スーパーバイザパスワード入力画面が表示されます。
インストール時に設定したスーパーバイザパスワードを入力し、［OK］をクリックしてください。

3. 設定のご案内が表示されます。［次へ］をクリックしてください。

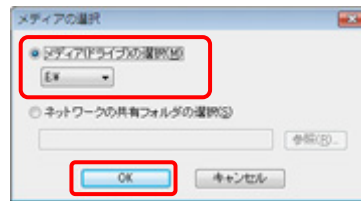
4. パソコンの鍵の作成に関する説明が表示されます。
内容を確認して準備ができたら、[次へ]をクリックしてください。

5. ［パソコン用の鍵を新規作成］が選択されています。ドライブ一覧に、内蔵ハードディスクドライブ以外のドライブが表示されている場合はチェックをはずしてください。
鍵を作成するメディアを装着し、[次へ]をクリックしてください。

Notice

- システムドライブのチェックは外せません。
- 内蔵ハードディスクドライブは必ずチェックしてください。
内蔵ハードディスクドライブのチェックを外すと、その内蔵ハードディスクドライブへのデータのコピー、移動およびファイルの新規作成ができなくなったり、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しなくなったりする場合があります。
- 内蔵ハードディスクドライブではないドライブのチェックは必ずはずしてください。
内蔵ハードディスクドライブではないドライブにチェックをつけると、そのドライブを取り外した際に動作が不正になる場合があります。

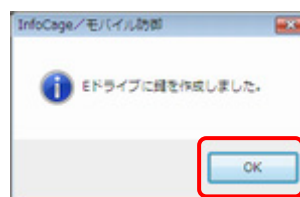
6. [鍵を格納するメディアまたは共有フォルダ]の[選択]をクリックしてください。

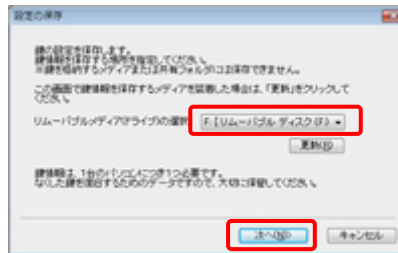
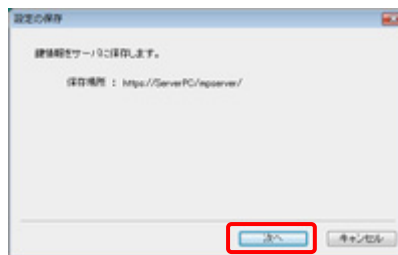
Notice

以下では 1 つの鍵を作成する方法を説明します。
合成鍵を作成する場合は、「InfoCage モバイル防御 ユーザーズガイド」の「合成鍵を作成する」の項を参照してください。(合成鍵は Windows XP/2000 のみ作成できます。)

7. ［メディア（ドライブ）の選択］を選択し、ドライブ一覧から鍵を作成するメディアのドライブを選択して［OK］をクリックしてください。
（ここでは例として E ドライブとします）

8. ［次へ］をクリックしてください。

9. 内容を確認後、［作成］をクリックしてください。

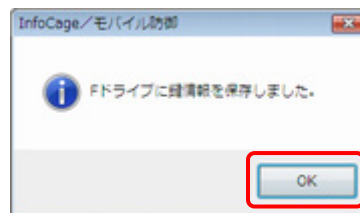
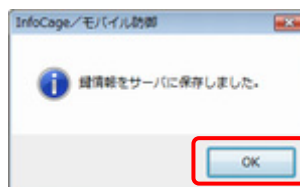
10. 鍵の作成が完了しました。［OK］をクリックしてください。

11. 続いて鍵情報を保存します。

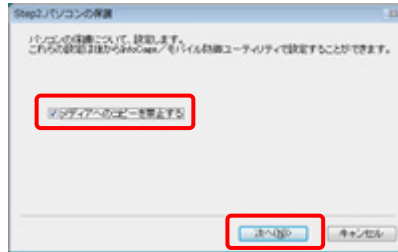
＜スタンドアローンモードの場合＞
鍵情報を保存するメディアを装着してください。
（ここでは例としてＦドライブに保存します）
外部メディア（ドライブ）一覧に鍵情報を保存するメディアが見つからない場合は、［更新］をクリックしてください。
鍵情報の保存先メディアを選択し、[次へ]をクリックしてください。

＜ネットワークモードの場合＞
鍵情報をサーバに保存します。保存場所を確認して、[次へ]をクリックしてください。

Notice

認証に失敗した場合は、以下を参照してください。

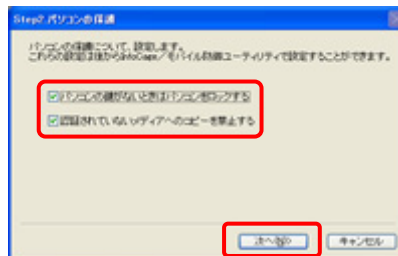
第 11 章 トラブルシューティング (2)

12. 鍵情報の保存が完了しました。[OK]をクリックしてください。

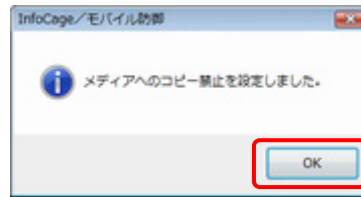
＜スタンドアローンモードの場合＞

＜ネットワークモードの場合＞

13. パソコンの保護に関する設定画面が表示されます。

＜Windows Vista の場合＞
データの抜き取り防止設定をする場合は、[メディアへのコピーを禁止する]のチェックを入れて[次へ]をクリックしてください。

Notice

- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、[メディアへのコピーを禁止する]は操作できません。
- 外部メディア自動暗号が無効になっている場合、ここにチェックをするとすべての外部メディアへのデータのコピーができなくなります。

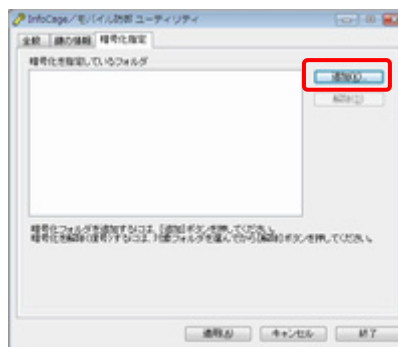
＜Windows XP/2000 の場合＞
あらかじめ[パソコンの鍵がないときはパソコンをロックする]にチェックが入っています。
データの抜き取り防止設定をする場合は、[認証されていないメディアへのコピーを禁止する]のチェックを入れて[次へ]をクリックしてください。

Notice

- 通常は[パソコンの鍵がないときはパソコンをロックする]のチェックを入れて使用してください。
  このチェックを外す場合は、「InfoCage モバイル防御 ユーザーズガイド」の「パソコンのロック」の項を参照してください。
- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、[認証されていないメディアへのコピーを禁止する]はチェックできません。

14. 設定内容の確認画面が表示されます。[OK]をクリックしてください。

Notice

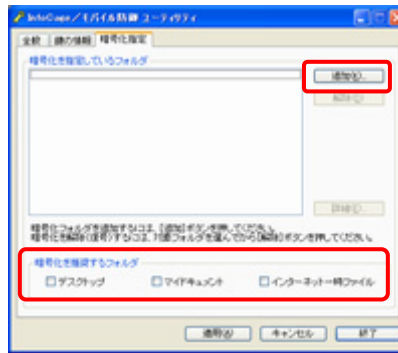
- 設定内容によっては、上記の画面に表示される内容が異なる場合があります。
- これ以降、設定内容が適用されます。
  Windows Vista の場合、メディアへのコピーを禁止した場合は、メディアへの書き込みができません。
  Windows XP/2000 の場合、パソコンをロックする設定をした場合は、鍵を抜くとパソコンがロックされます。ロックを解除し、ログオンするには鍵を装着してください。
  また、認証されていないメディアへのコピーを禁止した場合は、認証されていないメディアへの書き込みができません。

15. 暗号化指定に関する説明が表示されます。
内容を確認して準備ができたら、[次へ]をクリックしてください。

16. [暗号化指定]タブが表示されます。[追加]をクリックしてください。

＜Windows Vista の場合＞

Notice

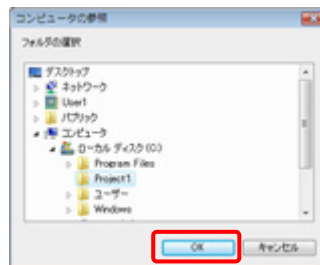
- InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが[暗号化を指定しているフォルダ]に表示されています。
- 他に暗号化設定するドライブやフォルダがない場合は、*18* へ進んでください。

<Windows XP/2000 の場合>

以下のフォルダを暗号化する場合は、［暗号化を推奨するフォルダ］内のチェックボックスにチェックを入れてください。

・デスクトップ　　　　・マイドキュメント　　　・インターネット一時ファイル

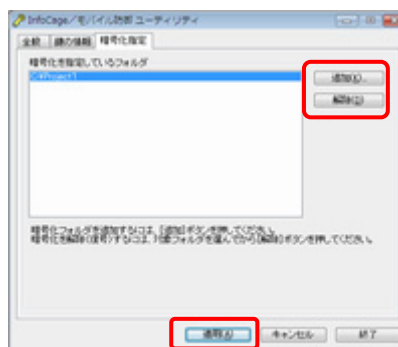
Notice

- デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合はデスクトップの任意の場所をクリックし、［F5］キーを押すと正常に戻ります。また、アイコンの並びが変更される場合がありますが、その場合は手動で並び替えてください。
- InfoCage モバイル防御　管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが［暗号化を指定しているフォルダ］に表示されています。
- 他に暗号化設定するドライブやフォルダがない場合は、*18* へ進んでください。

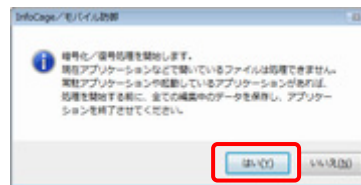
17. 暗号化したいドライブまたはフォルダを選択し、［OK］をクリックしてください。

18. ［暗号化を指定しているフォルダ］に選択したフォルダが追加されます。

複数のフォルダを指定したい場合は、*16* ～ *17* を繰り返してください。

また、暗号化したいドライブおよびフォルダを解除する場合は、［解除］をクリックしてください。

ドライブやフォルダを指定し終わったら［適用］をクリックしてください。

⚠Notice

- すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、それらを[解除]後、[適用]または[終了]を実行するとそれらのフォルダは復号されますのでご注意ください。
- [適用]をクリックすると、暗号化処理が終了するまで暗号化指定しているドライブおよびフォルダにはアクセスできなくなります。([一時停止]をクリックしても同様です)
- ここで[終了]をクリックすると、指定したドライブおよびフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

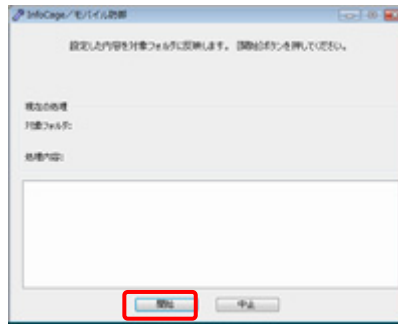
19. 暗号化処理に関する注意事項が表示されます。
常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、[はい]をクリックしてください。

⚠Notice

アプリケーションが使用しているファイルは、暗号化できない場合があります。

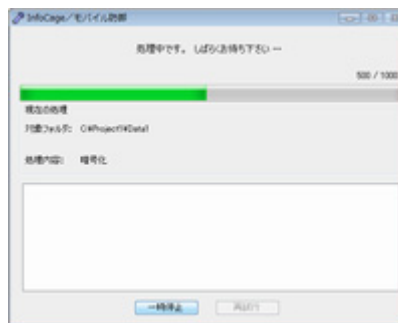
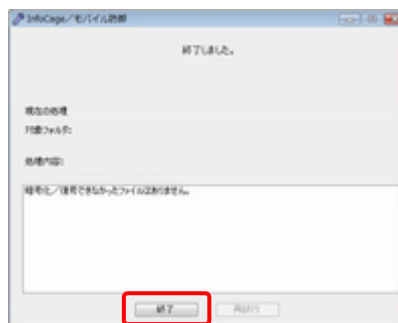
20. ごみ箱の暗号化に関する注意事項が表示されます。
内容を確認して、[OK]をクリックしてください。

⚠Notice

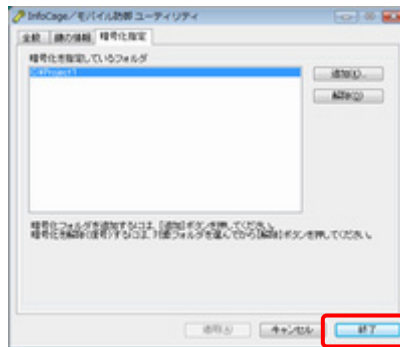
- 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

21. [開始]をクリックすると、暗号化処理が始まります。

⚠Notice

暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

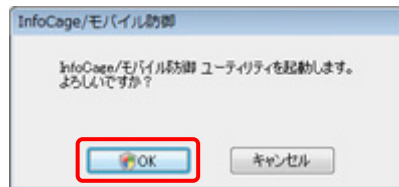
22. 暗号化処理中です。しばらくお待ちください。

23. 暗号化処理が終了しました。暗号化できなかったファイルがある場合はウィンドウ内に表示されます。
[終了]をクリックしてください。

⚠Notice

- 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、[再試行]をクリックしてください。
  すべての起動中のアプリケーションを終了して[再試行]をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、動作に問題はありません。
- 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
- 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」タブ」の項を参照してください。

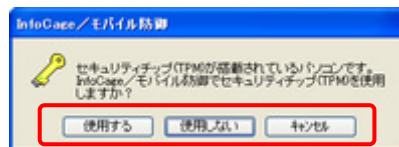
24. [暗号化を指定しているフォルダ]に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。[終了]をクリックしてください。

その他の設定に関しては、「InfoCage　モバイル防御　ユーザーズガイド」を参照してください。

4.2 パスワード認証方式の場合

Operation

1. Windows Vista の場合は再起動後に、以下の画面が表示されます。
[OK]をクリックしてください。

Notice

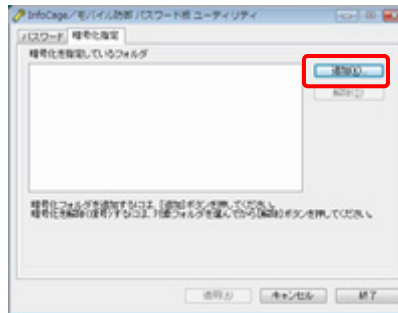
［キャンセル］をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを起動して、パソコンの鍵を作成および暗号化を行ってください。

2. Windows XP の場合、セキュリティチップ(TPM)搭載のパソコンをお使いでセキュリティチップ(TPM)が有効になっていると、InfoCage モバイル防御の管理者の設定によっては、下記の画面が表示される場合があります。

セキュリティチップ(TPM)を使用する場合は［使用する］を、使用しない場合は［使用しない］を、後で選択する場合は[キャンセル]をクリックしてください。
［キャンセル］をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御ユーティリティの起動時にメッセージが表示されます。

Notice

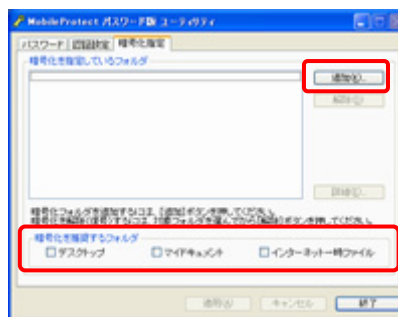
セキュリティチップ(TPM)に関しては、本ガイドの「第 10 章 セキュリティチップ(TPM)搭載のパソコンをお使いの場合」を参照してください。

3. 暗号化処理に関する説明が表示されますので、必ず内容を確認し、[OK]をクリックしてください。

4. [暗号化指定]タブが表示されます。[追加]をクリックしてください。

＜Windows Vista の場合＞

⚠Notice

- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドライブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、外部メディアと同じ扱いとなり、その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなります。
  また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。
- InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが[暗号化を指定しているフォルダ]に表示されています。
- 他に暗号化設定するドライブやフォルダがない場合は、*6* へ進んでください。

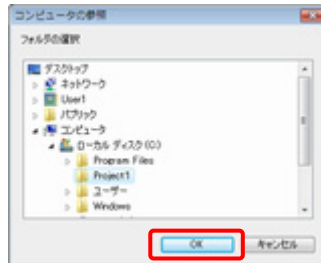
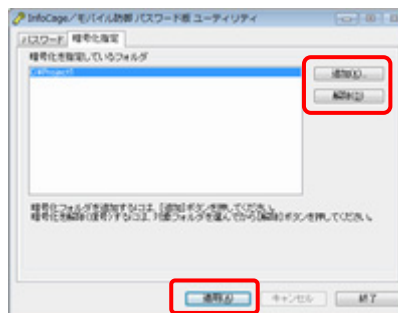
＜Windows XP/2000 の場合＞

以下のフォルダを暗号化する場合は、[暗号化を推奨するフォルダ]内のチェックボックスにチェックを入れてください。

・デスクトップ　　　・マイドキュメント　　・インターネット一時ファイル

⚠Notice

- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドライブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、外部メディアと同じ扱いとなり、その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなります。また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。
- デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合はデスクトップの任意の場所をクリックし、[F5]キーを押すと正常に戻ります。また、アイコンの並びが変更される場合がありますが、その場合は手動で並び替えてください。

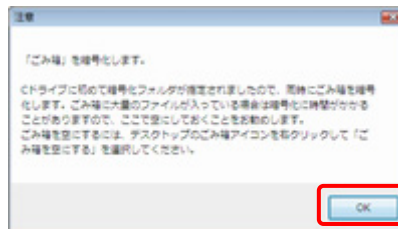
- 管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが[暗号化を指定しているフォルダ]に表示されています。
- 他に暗号化設定するドライブやフォルダがない場合は、*6* へ進んでください。

5. 暗号化したいドライブまたはフォルダを選択し、[OK]をクリックしてください。

6. [暗号化を指定しているフォルダ]に選択したフォルダが追加されます。
複数のフォルダを指定したい場合は、 *4* ～*5* を繰り返してください。
暗号化したいドライブおよびフォルダを解除する場合は、[解除]をクリックしてください。
すべて指定し終わったら[適用]をクリックしてください。

Notice

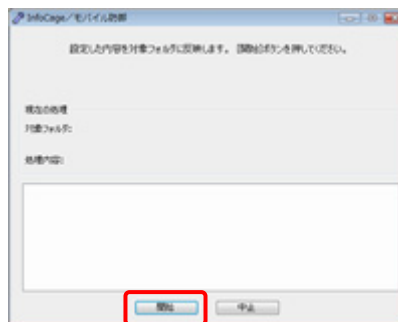
- すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、それらを[解除]後、[適用]または[終了]を実行するとそれらのフォルダは復号されますのでご注意ください。
- [適用]をクリックすると、暗号化処理が終了するまで暗号化指定しているフォルダにはアクセスできなくなります。(暗号化処理を実行中に[一時停止]をクリックしても同様です)
- ここで[終了]をクリックすると、指定したフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

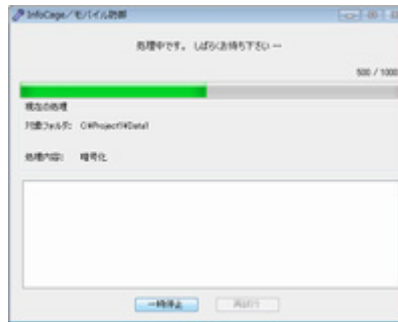
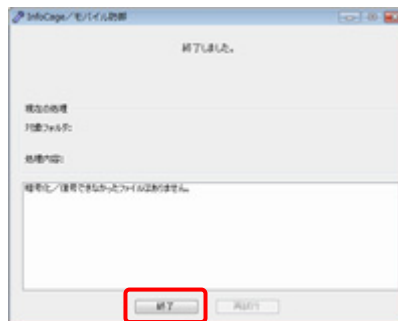
7. 暗号化処理に関する注意事項が表示されます。
常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、[はい]をクリックしてください。

⚠Notice
アプリケーションが使用しているファイルは、暗号化できない場合があります。

8. ごみ箱の暗号化に関する注意事項が表示されます。
内容を確認して、[OK]をクリックしてください。

⚠Notice

- 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
  またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

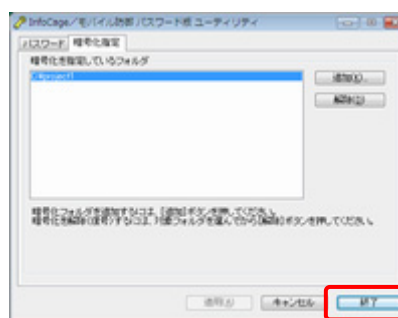
9. [開始]をクリックすると、暗号化処理が始まります。

⚠Notice
暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

10. 暗号化処理中です。しばらくお待ちください。

11. 暗号化処理が終了しました。
暗号化できなかったファイルがある場合はウィンドウ内に表示されます。
[終了]をクリックしてください。

⚠Notice

・ 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、[再試行]をクリックしてください。
すべての起動中のアプリケーションを終了して[再試行]をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、問題はありません。

・暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。

・ 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」タブ」の項を参照してください。

12. [暗号化を指定しているフォルダ]に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。[終了]をクリックしてください。

その他の設定に関しては、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

第5章 アップグレードインストール

Notice

Windows XP/2000 の場合、アップグレードインストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。

環境のチェック方法は、「3.2.1 環境チェックユーティリティ Windows XP/2000 の場合」を参照してください。

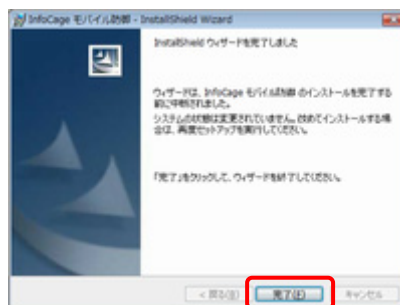
● **ご注意**

すでにインストールされている InfoCage モバイル防御と同じバージョンの setup.exe を実行するとアンインストールのウィザードが起動しますのでご注意ください。その際は下記の手順にしたがって操作してください。

Operation

1. setup.exe を実行すると、[InstallShield(R)ウィザードを使うと、InfoCage モバイル防御を削除することができます。]と表示された場合は、[キャンセル]をクリックしてください。

2. [はい]をクリックしてください。

3. [完了]をクリックしてください。操作は以上です。

アップグレードインストールを行います。

1. InfoCage モバイル防御が格納されているメディア(例 CD-ROM)内の setup.exe を実行し、[次へ]をクリックしてください。

2. インストールする InfoCage モバイル防御のプログラムの確認画面が表示されます。
[次へ]をクリックしてください。

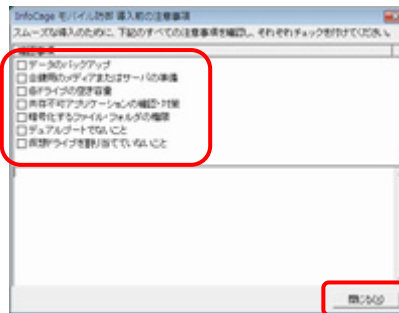
⚠ Notice

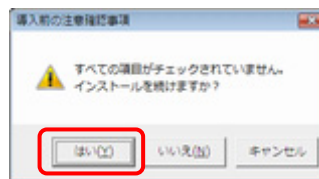
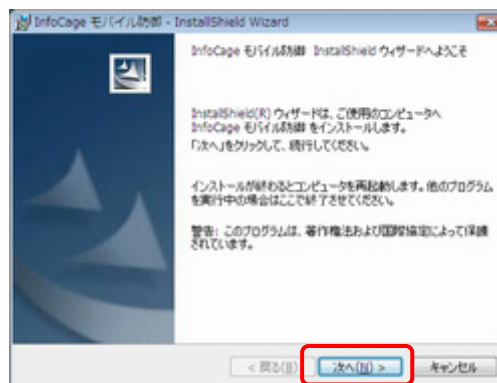
画面はメディア鍵認証方式版です。

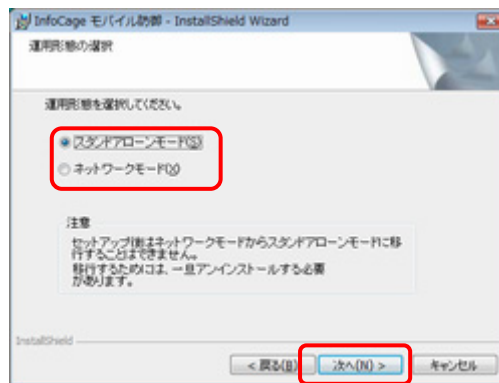
3. 確認メッセージが表示されます。[はい]をクリックしてください。

⚠ Notice

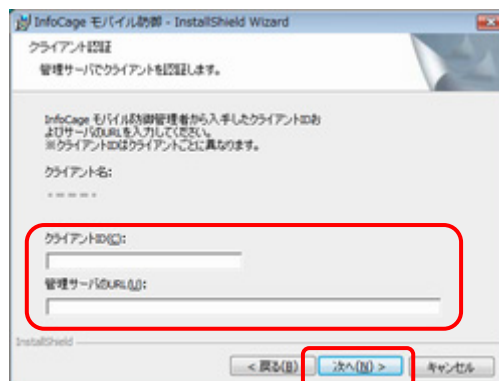
アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。

4. ［導入前の注意事項］画面が表示されます。
各項目をクリックすると詳細な説明が表示されますので、必ずお読みの上、チェックを付けてください。
すべての確認が終わりましたら、[閉じる]をクリックしてください。

> **⚠ Notice**
> 画面はメディア鍵認証方式の場合です。パスワード認証方式の場合は一部異なります。

5. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は［はい］を、インストールを中止する場合は［いいえ］を、*4* の画面に戻る場合は[キャンセル]をクリックしてください。

6. [次へ]をクリックしてください。

> **⚠ Notice**
> お使いのバージョンによっては[InfoCage モバイル防御用のInstallShieldウィザードを続行しています]と表示されますので、*7* または *9* または *10* へ進みます。

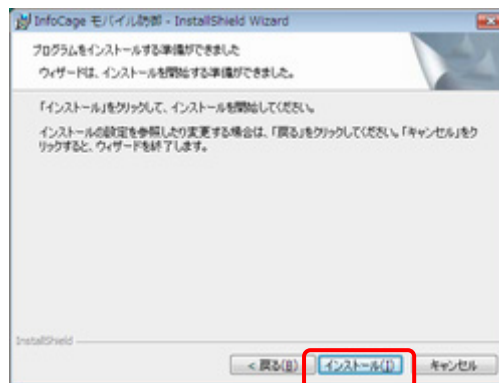
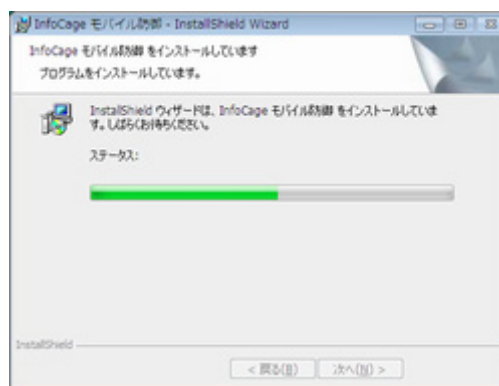
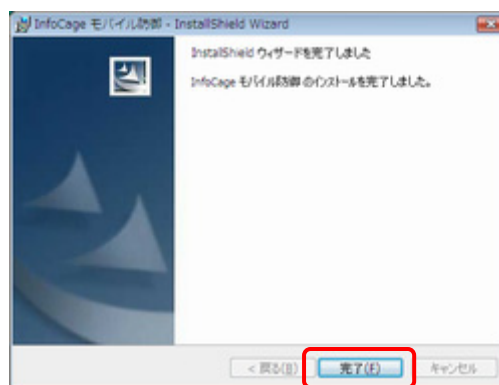
7. ［運用形態の選択］画面で、運用形態の選択をし、[次へ]をクリックします。

⚠Notice

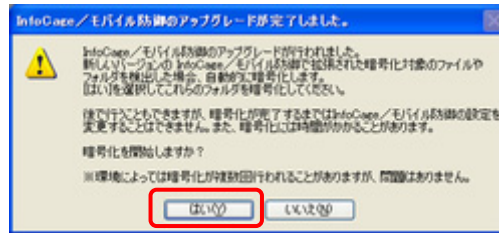
- アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。
- スタンドアローンモードを選択した場合は *9* へ。

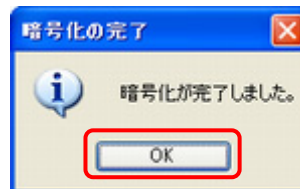
8. ≪ネットワークモード≫を選択した場合、クライアント認証画面が表示されるので、クライアント ID、管理サーバの URL を入力して、[次へ]をクリックしてください。

⚠Notice

- アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。
- スタンドアローンモードの場合、この画面は表示されません。
- InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。
  認証に失敗した場合は、クライアント名、クライアント ID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。
- その他の理由で認証に失敗した場合は、以下を参照してください。

参照 第 11 章 トラブルシューティング (2)

9. [インストール]をクリックしてインストールを開始してください。

10. インストール中です。しばらくお待ちください。

11. インストールが完了すると下記の画面が表示されます。
[完了]をクリックしてください。

12. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。
他のプログラムを実行中の場合は、終了させてください。
[OK]をクリックすると、パソコンが再起動します。

13. Windows XP/2000 の場合、お使いのバージョンによっては、再起動後に表示されるパスワード入力画面でスーパーバイザパスワードまたはユーザパスワードを入力すると、下記のメッセージが表示される場合があります。内容を確認し、[はい]をクリックしてください。

> **⚠ Notice**
>
> 暗号化を後で行う場合は[いいえ]をクリックしてください。
> [いいえ]をクリックした場合、暗号化が完了するまでは InfoCage モバイル防御 ユーティリティを起動するごとにメッセージが表示されます。

14. 暗号化が完了すると下記のメッセージが表示されますので、[OK]をクリックし、InfoCage モバイル防御 ユーティリティを終了してください。

以上で操作は完了です。

第6章 ログオン方法

InfoCage モバイル防御をインストールすると、Windows のログオン方法が変わります。
以下を行うことでセキュリティ認証を行い、Windows へログオンしてパソコンを操作できるようになります。

● **メディア鍵認証方式の場合**

鍵となるメディア等をパソコンに装着することでセキュリティ認証を行います。
(鍵となるメディア等は、鍵の作成の完了後に装着が必要となります。
InfoCage モバイル防御のインストール後に初めて Windows にログオンする際は、通常のログオンとなります。)

● **パスワード認証方式の場合**

InfoCage モバイル防御のユーザパスワードを入力することでセキュリティ認証を行います。

以下の手順で Windows へログオンします。

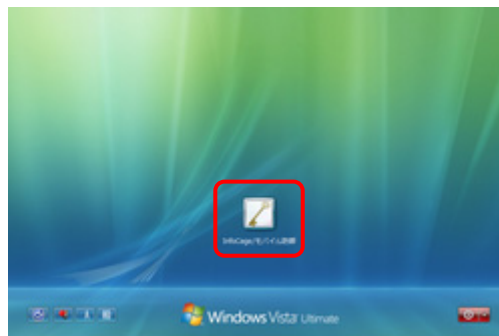
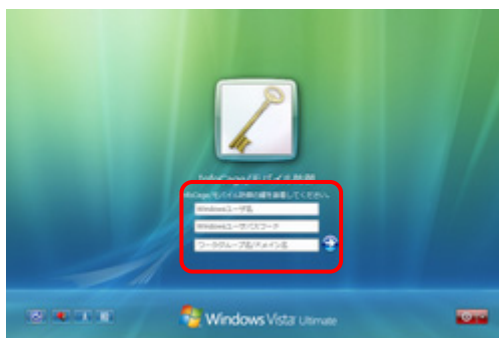
6.1 メディア鍵認証方式の場合

起動しているパソコンから鍵を抜いた場合、または鍵を抜いたままパソコンを起動した場合は、パソコンがロックされた状態になります。

Notice

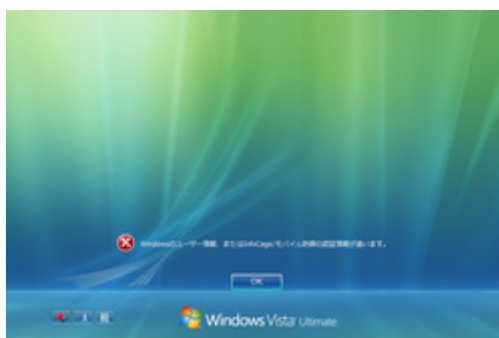
- 鍵を作成していない場合は、パソコンをロックできません。
- パソコンのロック機能のみでは情報漏洩対策は万全ではありません。重要なファイルは必ず暗号化してください。
- ネットワークの共有フォルダの鍵を使用する場合は、InfoCage モバイル防御のセキュリティ認証からWindows へログオンしてください。他の認証方法で Windows へログオンした場合はいったんログアウトし、InfoCage モバイル防御のセキュリティ認証からログオンしなおすと、シャットダウン時までネットワークの共有フォルダの鍵が有効になります。

■ Windows Vista の場合

1. InfoCage モバイル防御のボタンをクリックします。

2. 鍵となるメディアをパソコンに装着して Windows のユーザ名およびパスワードを入力して をクリック、または Enter キーを押すと、Windows へログオンすることができます。

⚠Notice

ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。
（ワークグループの場合は空欄でも可。）

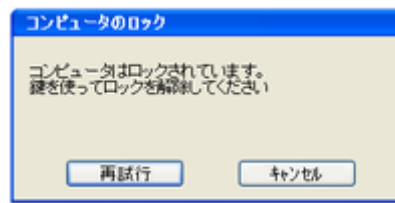
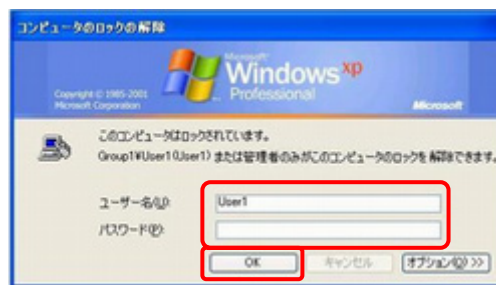
●ユーザ情報エラーの場合

メディア鍵認証方式の場合は鍵を抜いた状態、パスワード認証方式の場合は誤ったユーザパスワードでログオンしようとすると、[Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。] と表示され、Windows へログオンできません。
[OK]をクリックして、*2* に戻って操作してください。

■ Windows XP/2000 の場合

● 起動しているパソコンから鍵を抜いた場合

1. 起動しているパソコンから鍵を抜くと、[コンピュータのロック] 画面が表示され、パソコンがロックされた状態になります。

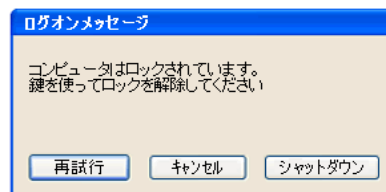
> **⚠ Notice**
> Windows の設定によっては、[コンピュータのロック]画面は表示されない場合があります。

2. 鍵を抜いた状態でログオンしようとすると、以下の画面が表示され、ログオンできません。

3. 鍵を装着して[再試行]をクリックすると、[コンピュータのロックの解除]画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

● 鍵を抜いた状態でパソコンを起動した場合

1. パソコンを起動すると[Windows へようこそ]画面が表示されます。

⚠Notice

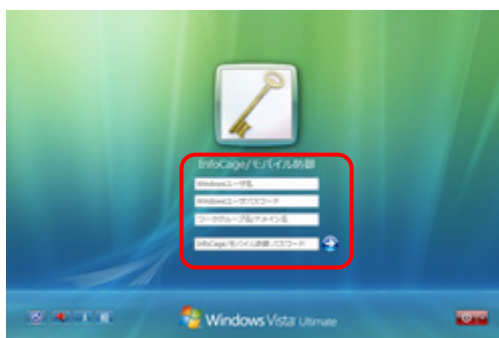
Windows の設定によっては、[Windows へようこそ]画面は表示されない場合があります。

2. 鍵を抜いた状態でログオンしようとすると、以下の画面が表示され、ログオンできません。

3. 鍵を装着して[再試行]をクリックすると、[Windows へログオン]画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

6.2 パスワード認証方式の場合

■ Windows Vista の場合

1. InfoCage モバイル防御のボタンをクリックします。

2. Windows のユーザ名およびパスワード、InfoCage モバイル防御のユーザパスワードを入力して をクリックするか、Enter キーを押すと、Windows へログオンすることができます。

> **⚠ Notice**
>
> ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。
> (ワークグループの場合は空欄でも可。)

●ユーザ情報エラーの場合

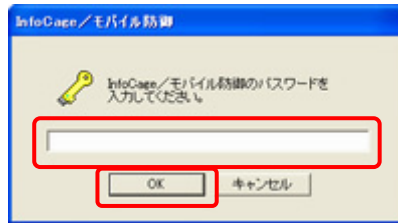
誤ったユーザパスワードを入力すると、[Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。] と表示されログオンできません。
[OK]をクリックして、*2* に戻って操作してください。

> **Notice**
>
> ユーザパスワードを 5 回誤って入力すると、パソコンがロックアウトされます。その場合はパスワード入力画面が有効になるまでしばらくお待ちください。

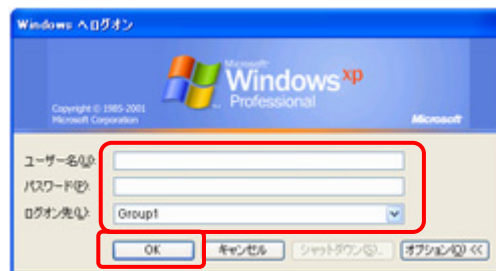
■ Windows XP/2000 の場合

1. 再起動後に、通常のログオン画面が表示されます。
Ctrl＋Alt＋Del キーを押してください。

> **Notice**
>
> Windows の設定によっては、[Windows へようこそ]画面は表示されない場合があります。

2. ユーザパスワード入力画面が表示されます。
インストール時に設定したユーザパスワードを入力し、[OK]をクリックしてください。

⚠Notice

ユーザパスワードを 5 回連続で誤って入力すると、[OK]がクリックできなくなります。
その場合は ［シャットダウン］ をクリックしていったんシャットダウンした後、再度パソコンを起動してパスワード入力画面が有効になるまでしばらくお待ちください。
（すぐにパソコンを起動しても一定時間パスワードの入力はできません。）

3. [Windows へログオン]画面が表示され、ユーザ名と Windows ログオンパスワードを入力すると
ログオンすることができます。

第7章 特定の FeliCa カードの設定

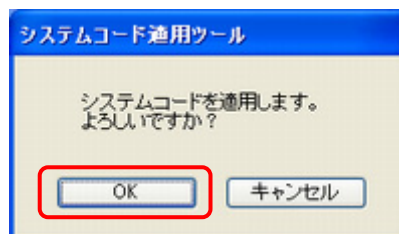
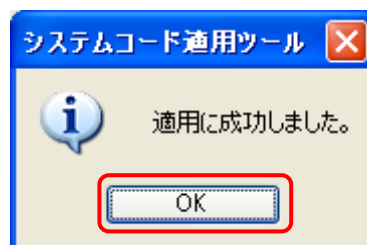
Windows XP/2000 の場合、InfoCage モバイル防御をパスワード認証方式で運用しログオン認証に特定の FeliCa カードを使用するためには、システムコード(FeliCa カードに割り当てられている固有のコード)を適用する必要があります。
インストール後にシステムコードを適用する場合は、システムコード適用ツールを使用します。
本設定は InfoCage モバイル防御の管理者の指示にしたがって操作してください。

Notice

- 本ツールは Windows XP/2000 用の InfoCage モバイル防御 Ver3.5 以降がインストールされたパソコンで動作します。Windows Vista 用 InfoCage モバイル防御には FeliCa 認証機能はありません。
- InfoCage モバイル防御の管理者によって FeliCa カードのシステムコードが設定されたセットアッププログラムでインストールした場合は、本設定は不要です。
- システムコード適用ツールは、コンピュータの管理者のユーザで実行してください。
- FeliCa カード認証は InfoCage モバイル防御をメディア鍵認証方式で運用している場合は使用できません。

Operation

1. InfoCage モバイル防御の管理者から配布された mbscd.dat ファイルを、InfoCage モバイル防御をインストールしたフォルダ(通常は ¥Program Files¥NEC¥InfoCageCE)内の¥Tools フォルダ内にある NmlStScd.exe と同じ場所に保存してください。

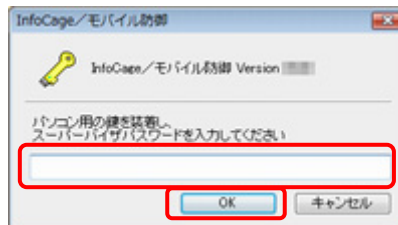
2. NmlStScd.exe を実行し、[OK]をクリックします。

3. システムコードが適用されました。[OK]をクリックしてください。

以上で終了です。
FeliCa カードの設定方法は、「InfoCage モバイル防御 ユーザーズガイド」の「「認証設定」タブ」の項を参照してください。(パスワード認証方式のみ)

第8章 ユーティリティの起動方法

InfoCage モバイル防御 ユーティリティの起動方法を説明します。

1. スタートメニューから、[すべてのプログラム]－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーティリティ]をクリックします。

2. Windows Vista の場合は以下の画面が表示されます。
[OK]をクリックしてください。

3. メディア鍵認証方式の場合は、鍵をパソコンに装着してからスーパーバイザパスワードを入力し、[OK]をクリックしてください。
パスワード認証方式の場合は、ユーザパスワードを入力し、[OK]をクリックしてください。
InfoCage モバイル防御ユーティリティが起動します。

Notice
上記の画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部表記が異なります。

● **InfoCage モバイル防御 ユーザーズガイドを参照するには**

スタートメニューから、[すべてのプログラム]－[NEC]－[InfoCage モバイル防御]－[InfoCage モバイル防御 ユーザーズガイド]をクリックしてください。

第9章　時限消去機能について

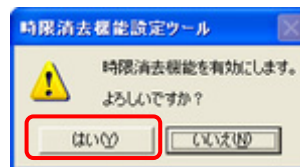
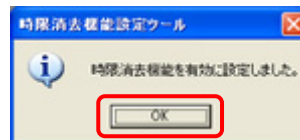
時限消去機能を使用するためには[時限消去機能設定ツール]で有効にする必要があります。
以下の手順にて有効にしてください。

Notice

- 時限消去機能は Windows XP/2000 のみの機能です。
- InfoCage　モバイル防御がインストールされたパソコン上での操作手順です。

Operation

1. クライアント CD-ROM 内の¥2K_XP¥Tools¥時限消去機能設定ツール　フォルダにある EnableTBM.exe を実行してください。

2. メッセージが表示されますので[はい]をクリックしてください。

3. [OK]をクリックしてください。

以上で終了です。
時限消去機能の設定方法は、「InfoCage　モバイル防御　ユーザーズガイド」の「「時限消去設定」タブ」の項を参照してください。

第10章 セキュリティチップ(TPM)搭載のパソコンをお使いの場合

セキュリティチップ(TPM: Trusted Platform Module)とは、PC プラットフォームにおけるセキュリティ技術の業界団体 TCG(Trusted Computing Group)が策定した仕様に準拠した IC チップで、これを使用することにより、様々なセキュリティ機能を利用することが可能になります。

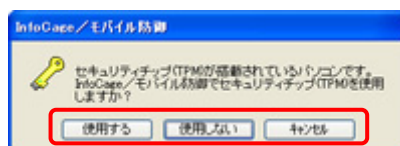
Windows XP をお使いの場合は、InfoCage モバイル防御のパスワード認証方式でセキュリティチップ(TPM)の機能を使用することにより、さらに強固なセキュリティを実現できます。
セキュリティチップ(TPM)を使用する場合は、InfoCage モバイル防御の管理者がカスタマイズしたセットアッププログラムを使ってインストールしてください。

■ セキュリティチップ(TPM)の使用について

セキュリティチップ(TPM)を有効に設定したセットアッププログラムを使ってインストールした場合は、セキュリティチップ(TPM)を使用するかを選択することができます。
セキュリティチップ(TPM)を有効にするには、BIOS セットアップでセキュリティチップを[使用する]にし、セキュリティチップユーティリティをインストールしてください。

⚠Notice

セキュリティチップ(TPM)の設定方法についてはお使いのパソコンのマニュアルを参照してください。

InfoCage モバイル防御のパスワード認証方式をインストール後、InfoCage モバイル防御 ユーティリティの起動時に下記のメッセージが表示されます。
セキュリティチップ(TPM)を使用する場合は[使用する]を、使用しない場合は[使用しない]を、後で選択する場合は[キャンセル]をクリックしてください。
[キャンセル]をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御 ユーティリティの起動時にメッセージが表示されます。

■ 注意事項

- セキュリティチップ(TPM)を使用するには、InfoCage モバイル防御のパスワード認証方式をインストールする前にセキュリティチップ用ドライバおよびユーティリティがインストールされている必要があります。
- BIOS のアップデートなどで設定値を初期化した場合、アップデート後にセキュリティチップの値を必ず元に戻してください。
- セキュリティチップ(TPM)を使用している場合、セキュリティチップユーティリティをアンインストールしないでください。アンインストールすると暗号化されたファイルにアクセスできなくなります。
- セキュリティチップ(TPM)を使用している場合、BIOS でセキュリティチップを[使用しない]に設定を変更したり、設定値の初期化をしたりすることは絶対にしないでください。これらの操作を実行した場合、暗号化されたファイルにアクセスできなくなります。

第11章 トラブルシューティング

(1) インストール時に「1607:InstallShield Scripting Runtime をインストールできません。」というメッセージが表示され、インストールできない。

このエラーは、InstallShield が次のような原因で正常に動作していないときに表示されます。

1. **管理者権限のないユーザでログオンしている。**
   インストールする際のユーザ権限は、コンピュータの管理者(Administrator 権限)で行ってください。

2. **IDriver.exe が正しく登録されていない。**
   Windows のコマンドプロンプトから以下のコマンドを実行して、IDriver.exe を登録しなおしてください。
   ¥Program Files¥CommonFiles¥InstallShield¥Driver¥7¥Intel32¥IDriver.exe/REGSERVER (注1)
   ※ Windows が C ドライブにインストールされている場合の例です。
   それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
   ※ 下線部はお使いの環境によって異なる場合があります。

3. **同時に複数のインストーラが起動している。**
   誤って setup.exe を複数実行してしまった場合、いったんすべてのインストーラを終了してから、再度インストールを行ってください。

4. **Windows インストーラ(msiexec.exe)が正しく登録されていない。**
   任意の場所(デスクトップ等)に[新規作成]でテキストファイルを作成し、ファイルの拡張子を.txt から.msi に変更してください。
   アイコンがインストーラのアイコンに変わるか確認します。アイコンがインストーラのアイコンに変わらない場合は、コマンドプロンプトで以下のコマンドを実行してください。
   C:¥Windows¥System32¥msiexec.exe /REGSERVER
   ※ Windows XP が C ドライブにインストールされている場合の例です。
   それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
   また、OS が異なる場合はシステムフォルダ名を置き換えてください。

5. **「SUBST」コマンドで作成した仮想ドライブからインストールを実行している。**
   SUBST コマンドによる仮想ドライブを解除してください。

(2) ネットワークモードの場合、管理サーバと通信できない、または管理サーバのクライアント認証に失敗する。

1. インストール時に使用したクライアント名、クライアント ID、管理サーバの URL が正しいか確認してください。
2. コマンドプロンプトで管理サーバに ping コマンドを実施してください。ping コマンドでエラーが発生した場合は、管理サーバとの通信が行われていない可能性があります。
   ※ ping についてはオペレーティングシステムのマニュアル等を参照してください。ネットワークで ping コマンドが禁止されている場合がありますのでご注意ください。また、OS が異なる場合はシステムフォルダ名を置き換えてください。
3. DNS 設定していない可能性があります。設定していない場合は、ネットワーク管理者に管理サーバの IP アドレスを DNS 設定してもらってください。
4. URL の管理サーバ名部分を IP アドレスに変更して接続すると、接続できる場合があります。

参照 その他については「InfoCage モバイル防御 ユーザーズガイド」のトラブルシューティングを参照してください。

InfoCage モバイル防御 Ver 3.61
インストールガイド

日本電気株式会社
東京都港区芝 5 丁目 7 番 1 号
TEL(03)3454-1111（大代表）

MI361-0801-01